IS Security Leveraging the Concept of Knowledge Management

Neville, Karen

Award date:
2010

Awarding institution:
University of Bath

PhD	2010	K. M. Neville

IS Security Leveraging the Concept of Knowledge Management

Karen Mary Neville BSc, MSc.

A thesis submitted for the degree of Doctor of Philosophy
University of Bath
School of Management
February 2010

Signed: ……

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

As a part-time student of the University of Bath and as a College Lecturer of University College Cork, I have many people to thank for the help and support they gave me as I conducted this research.

University College Cork, Ireland:

Professor Ciaran Murphy who has always provided me with a great deal of support and encouragement throughout my career and the PhD process.

Professor Frederic Adam who provided me with a great deal of time, guidance and feedback and without whom this research would not have been possible.

Patricia Lynch for all of the support and encouragement you have given me since I started in Business Information Systems and through the PhD process.

Thank you very much Simon Woodworth, John O'Donoghue and Joe Feller for the practice viva.

I know this thesis would never have been completed without the help of my colleagues and friends in the Department of Accounting, Finance and Information Systems. I would like to thank particularly the following for all of the 'PhD chats': Andrew Pope, Claire O'Sullivan Rochford, Margaret Healy, Niamh O'Riordan, Karen Hannigan, Ciara Heavin, Tom O'Kane, Mary Daly and Audrey Grace.

University of Bath, United Kingdom:

Professor George Philip and Dr. Steve Conway, my Viva Examiners and the first to read this thesis, I am very grateful for your feedback and particularly the discussions after the viva with Dr.Steven Conway from whom I learned a great deal – thank you.

Thank you Dr. Niki Panteli for your help, particularly, towards the end of this process. Chris Barns and Suzanne Swallows proved valuable sources of information and contacts for me for everything in the University of Bath.

Family & Friends:

To my friends who have supported and encouraged me throughout the PhD process – I appreciate everything you said and did. To Rosemary, Maria and Paula who have been my friends since primary school. The three of you have always and will always be incredibly important to me. Thank you Emily, who regularly checked to see if I was still alive while writing this thesis.

Last, but the most important: my family particularly my parents Patrick and Maureen – you have always inspired, encouraged and listened to me. I can never repay everything you have done for me. My brothers: John, Michael and Aidan who have always been very supportive and protective. My nephews Steve, Darren and niece Elle who took my mind off this thesis and cheered me up when I needed it.

Thank you everyone,
Karen

ABSTRACT

IS Security (ISS) has become a key element of business risk management and can itself create competitive advantage. Thus, organisations seek practical approaches to protect the operation of the business. Protecting the functionality of an organisation is a difficult task but it is the responsibility of both senior management and ISS functions to do so. An analysis of the ISS literature reveals a paucity of research of ISS management, and a need for research to develop a holistic model for managing ISS knowledge to overcome the ever-increasing number of negative security incidents. The ISS research community is restrained by small-scale technical questions as the social aspects of ISS are ignored resulting in fragmented research across the IS field. While several possible methods are scattered throughout the literature – they focus on the development of information systems. ISS professionals require a range of skills encompassing business knowledge, legal awareness, and organisational processes as well as technical security knowledge. Research to date has failed to provide an integrated approach to managing ISS knowledge.

This study investigates how ISS could leverage the concept of knowledge management. It proposes a theoretical model derived from the ISS and KM literatures. Thus to address this gap in research, this study adopts an exploratory interpretive holistic case study approach using interviews and document analysis as data gathering methods. The study will focus on the relationship between ISS and KM and the proposed benefits that an ISS KM initiative would produce. An analysis of the approaches used by these specialised structures in managing knowledge within and across the two case studies facilitated the development of an integrated model. The interplay between the functions provided rich description of the approaches used to manage knowledge. This research builds on previous studies documented in the ISS literature, by providing a much needed model against which practitioners may diagnose problems, plan action and implement solutions. ISS models and standards today do not exhibit much flexibility, therefore managers make ISS decisions in a vacuum. ISS problems can be managed or reduced when the ISS functions and management are aware of the full range of controls available and implement the most effective. Unfortunately, they often lack this knowledge and their subsequent actions to cope with threats are less effective.

The focus of ISS research to date has been technical and grounded in positivism and few, if any, studies utilise a qualitative approach, therefore eliminating holistic, in-depth rich descriptions of core issues within the field. Comparatively little work has taken a managerial point of view, covering broad organisational and social issues. This study acknowledges these issues and provides a solid conceptual foundation for future studies on ISS by answering calls for a theoretical model to guide research in the area. The study also identifies the positive and negative impacts of compliance and describes how organisations can apply the model to overcome these negative effects.

CHAPTER ONE

THE IS SECURITY CHALLENGE

1.0 Introduction

This Chapter highlights the scarcity of, and need for, research to develop a holistic model for managing IS Security knowledge to overcome the ever-increasing number of negative security incidents. Section 1.1 highlights the negative consequences of deficiencies in IS Security and the importance of knowledge of risks and threats. Section 1.2 defines IS Security, knowledge management and organisations as the Chapters of this thesis are implicitly rooted in these definitions. Section 1.3 presents the research objective and the research questions. The section also provides an overview of the relevance and rigour of the study. The section explains how this study extends the body of empirical evidence by developing a model consisting of people, processes and technology. Section 1.4 describes and illustrates the organisation of the thesis. Finally Section 1.5 concludes the Chapter.

1.1 Studying IS Security in Organisations

In just a few decades, the use of IT/IS has formalised information management and streamlined the administration of organisations (Galliers & Newell, 2001; Dhillon, 2006). The significance of IS Security for an organisation is proportional to the organisation's dependence on information. Therefore adequate IS Security is an enabler for inter-organisational relationships (Keen et al., 2000) and information management. An organisation's IS Security affects not only the organisation itself, but also its external parties (Von Solms, 1999). The more sensitive information an organisation handles the more important are confidentiality, integrity and availability. Deficiencies in IS Security can cause direct negative consequences for business processes due to errors, delays and information leakage. Organisations encounter numerous IS Security challenges, such as (Booz et al., 2005; Dhillon, 2006): a rapid expansion of the enterprise ecosystem through external partnerships and new global markets, a value migration from the physical to information-based and intangible assets, continuing pressure to reduce costs, and new security technologies such as biometrics are blurring functional boundaries and compliance regimes. To make effective decisions regarding IS Security, management must know about the various threats facing the organisation, its employees, data, information, knowledge and systems. Thus, knowledge of threats and attacks are crucial to management when allocating resources, formulating security policies and performing risk assessments (Jones & Ashenden, 2005). Failures in IS Security can temporarily deny network resources to employees and hackers can then use one organisation's resources as a stepping-stone in attacking another organisation.

1.2 IS Security and KM Definitions

Three families of definitions are required to map out the conceptual territory of this investigation: organisations, IS Security and knowledge management. The arguments in the following Chapters are implicitly rooted in these definitions.

The study of organisations is complex, as their processes are made up of many activities (Stamper, 1973; Nutt, 1984; Baskerville, 2004). Traditionally organisations have been viewed as formal systems concerned with inter-organisational (between the organisations and its environment) and intra-organisational (internal departments) information. Since computer-based systems have been used to automate the activities of these formal systems this view has evolved. The emergent belief of a number of studies is to view the organisation as an evolving or emerging social form (Baskerville, 2004; Dhillon, 2006). Consequently, the organisation allows different groups to interact with each other and the environment (Walsham, 1993).

Organisations and the functional areas within them evolve and the result is rarely a neat arrangement of employees and procedures (Strassman, 1995). Galliers and Baker (1994) observed that organisations often adopt mixtures of arrangements that can be difficult to study, creating problems for researchers of organisations. Organisational environments can be viewed as being composed of the informal, formal and technical interconnecting parts (Liebenau & Backhouse, 1990) or systems (Dhillon, 2006). Emergent organisations endure continuous change which is beyond simple environmental adaptiveness, allowing them to operate effectively in highly competitive markets by maintaining continual agility (Siponen & Iivari, 2006). Vulnerabilities and threats emerge as these organisations and their information systems are remade (Baskerville, 2004). As a result the context of IS Security is changing. Consequently, IS Security managers will need to manage the increasingly complex infrastructure - necessary to support and protect an emergent organisation. In order to provide the groundwork for such management IS Security researchers "...need to develop organisational approaches and methodologies that respond to this new context by providing techniques for supporting emergent security" (Baskerville, 2004, p.156). Emergent IS Security must cope with rapid changes in the organisation, shifting information systems and changing vulnerabilities and threats through the development of an integrated and agile approach to managing IS Security. Agile IS Security management is required to anticipate threats and rapid responses. Traditional IS Security management principles and approaches will endure in organisations which are static and non-competitive, protecting traditional systems from traditional threats.

IS Security is a complicated concept and field. The terms computer security, IT security, information security and information systems security (and their extensions) are often used interchangeably. The nature of security makes it difficult to measure and assess as it concerns phenomena that may not happen now but could happen in the future or which are occurring on an ongoing basis. Additionally, in contrast to other organisational processes and functions, such as productivity and sales, security is difficult to measure or even to judge objectively (Jonsson, 1995). It is only in isolated environments, where only technical aspects are considered, that measurements are applicable (ibid.). However IS Security deals with aspects other than technology, such as organisational processes and people. Frameworks for assessments and measurements of IS Security, both by practitioners (Veriscan, 2006) and academics, have been developed (Johansson, 2005; Randere, 2006). These were limited to technical aspects of IS Security such as incidents within corporate networks, and neglecting other factors that affect IS Security, such as the value of information assets and threats. The indirect consequences of security incidents also contribute to abstractness because they are so difficult to survey. An incident can lead to specific damage but its further spreading is difficult to foresee due to the fuzzy interfaces between information systems and organisations. As a result, it is difficult for organisations to estimate the level of IS Security for information systems, infrastructures and business partners. Encryption

technologies, firewalls, intrusion detection software (IDS) and virtual private networks (VPN) are all examples of complex technologies and applications that are difficult for non-experts to understand (Stewart, 2005). These technologies can be used to fragment organisational information systems into security compartments (Baskerville, 2004; Dhillon, 2006) within dynamic environments.

IS Security is an important issue for organisations. However it is an area that is difficult to grasp and estimate. The significance of IS Security motivates research and practical developments from a number of perspectives; technological, organisational and behavioural. The management of IS Security goes beyond allocating controls to objects but involves the people, processes and technologies of the organisation as a whole. It encapsulates every aspect from decision-making and environmental considerations to the overall objectives of the organisation. Therefore, for the purpose of this study, the following are put forward as working definitions of IS Security and knowledge management as a lens through which IS Security is investigated: *IS Security is a process that ensures the protection of information resources encompassing the people, processes and technologies used*.

Knowledge management (KM) *is concerned with ensuring that the knowledge is available in the right form to the right processors* [systems, people and processes] *whenever required*. It is a holistic attempt to manage organisational assets which are composed of people, technology and processes. KM consists of such processes as: knowledge acquisition (Alvi & Leider, 2001), capture (Becerra-Fernandez et al., 2004), creation (Oppong et al., 2005), sharing (Grant, 1996), application/use (Holsapple & Joshi, 2004) and control (Jamieson & Handzic, 2004). Technology, while a key enabler for both IS Security and KM, is not the primary driver in either initiative (Blacker, 1995; Siponen, 2005). As explained by existing theory IS Security plays a significant role regarding KM when technology is a factor (Jamieson & Handzic, 2004) or in controlling knowledge (Holsapple & Singh, 2004; Randeree, 2006). Access controls determine who has access to the different knowledge repositories and this has significant repercussions in KM as it can determine the value of the knowledge (Jamieson, 1991; Holsapple & Joshi, 2000; Jamieson & Handzic, 2004). The conviction within the KM community is that eighty percent of KM is composed of people and culture, and twenty percent is technology (Liebowitz & Chen, 2004).

Therefore IS Security plays a significant role in every tenet of KM to assure its validity and utility. It should be mapped to KM roles, culture, processes and technology and warrants additional research to investigate the relationship between both fields and to build on existing KM and IS Security theory. Gaps exist in the knowledge management and the IS Security literatures where a relationship between the fields has not been investigated (Belsis, et al., 2005; Jamieson & Handzic, 2004; Holsapple & Singh, 2004; Randeree, 2006). Although security is put forward as a necessary consideration in the design and implementation of knowledge management systems (KMS) (Eppler, 2004; Butler & Murphy, 2007), it is not identified as a consideration or aid in the management of knowledge, as in simply providing the right knowledge to the right people (logical access control). The IS Security literature advocates access controls, security policies, the integrity of information and environmental threats yet KM is ignored as an issue when it could be a solution.

The next section describes the research objective, questions and the contributions of this study.

1.3 Research Objective and Contribution

Lucas (1991) recommended that IS researchers should investigate interesting problems and underlying issues instead of focusing on the latest IS fashion. Therefore the primary objective of this study is:

> To explore how Information Systems Security (ISS) could leverage the concept of Knowledge Management (KM) through qualitative research.

To accomplish the research objective the following questions are proposed:

RQ.1: How can the organisational infrastructure support the management of IS Security (ISS) knowledge?

RQ.2: How do the two functional areas IS Security (ISS) and Customer Support (CS) manage knowledge?

RQ.3: How can firms align Information Systems Security (ISS) to a Knowledge Management (KM) environment?

1.3.1 The Relevance of this Study

Quality in IS research is measured through the relevance and rigour of the study (Keen, 1991). Knowledge development in the IS discipline should be useful for industry and not follow the latest fads and fashions (Galliers & Newell, 2001: 2003; Lucas 1991) or as Keen contends "...until relevance is established, rigour is irrelevant" (Keen, 1991 p.27). If a research result is useless, the rigour of the research is meaningless. The majority of research results must be applicable for practitioners otherwise IS research will degenerate into an introvert activity (Goldkuhl, 1996). The quality of this study, with regard to academia and practice, is discussed in the following section.

To make effective decisions regarding IS Security, management must know about the various threats facing the organisation, its employees, data, information, knowledge and systems (Jones & Ashenden, 2005). The effective management of IS Security is a knowledge-intensive activity that depends on the experience of IS Security experts. The effectiveness of current approaches to managing IS Security knowledge has been questioned given the volume of security breaches and well published security lapses such as: ChoicePoint, Bank of America, T-Mobile and LexisNexis. Management must not only minimise risks through the operationalisation of security activities but also effectively communicate vision, rules and guidelines to employees. Large volumes of data must be processed from a plethora of security technologies to provide information regarding the security landscape of the organisation (Stewart, 2005). As a result, management requires the development of an integrated approach to the management of security knowledge. Combining security activities, experts and tools could resolve these problems. This could be achieved through the utilisation of an effective KM approach. The application of the approach to the management of IS Security knowledge would enable a more holistic approach to the management of IS Security across the enterprise. Managerial environmental challenges are justification for the phenomenon under investigation. The adoption of adequate KM for IS Security knowledge will assure the convergence of IS Security across the enterprise. Chapter 2 addresses these issues in an attempt to clear up the conceptual confusion that persists in IS Security research, and in order to provide the study with a firm theoretical foundation.

The practical relevance of research findings differs from how the research has been conducted. Theoretical research can be enormously beneficial to practitioners while research conducted close to practice can be of little use for practitioners. If practitioners are involved in the research process, through for example open interviews and conversations, the researcher can be sensitive to their demands and needs. However, if a researcher undertakes studies close to practice; a greater understanding is developed of what problems are relevant and what research results are demanded by the practice. Research must of course be relevant for academics as well. This research examines the importance of IS Security in protecting the business and the development of an integrated approach to its management. The research contribution must have scientific readership and backing, in this case, from the IS Security research community.

The IS research community has embraced many technologies as the "silver bullet solution" to corporate information needs. This tendency could have serious implications and is leading to a disintegration of research and a lack of theoretical progression (Webster & Watson, 2002). This predisposition has had significant effects on IS Security research. IS Security is interlinked with every aspect of information systems, people and processes and therefore has consistently increased in importance in practice. The protection of corporate assets is a priority for organisations and investment in security has dramatically increased in the last ten years (Dhillon, 2006; Behara et al., 2007) due to new legislative requirements and the realisation that IS Security is a key enabler of business (CSI/FBI, 2007; Dhillon, 2006; Behara et al., 2007). However, the academic response to IS Security has resulted in a field that is theoretically underdeveloped. Previous IS Security research has been technical and conducted primarily by computer scientists, mathematicians, and computer engineers as criticised by leading IS researchers (Straub et al., 2008; Siponen & Willison, 2007; Dhillon, 2006). Similarly methods for the development of secure systems have been investigated (Baskerville, 1992; Siponen, 2005; Villarroel et al., 2005) while an integrated approach to managing IS Security has been ignored.

A recent survey argued that the number of IS Security research papers published in the leading IS journals such as MIS Quarterly, Information Systems Research, and the Journal of Management Information Systems has diminished (Siponen & Willison, 2007; Siponen et al., 2008). The researchers examined IS Security papers for the period 1990-2004; approximately one thousand and eighty were analysed in terms of theories, research methods and topics. One thousand and forty-three of the papers contained no theory. A large number of categories pertaining to IS Security were identified despite this large number; fourteen categories comprise seventy-two percent of all of the papers used in the study. The categories are summarised in Table 1.1. The focus of research has been technical even though it has long been recognised that it is as important to understand the social elements. Comparatively little work has taken a managerial point of view, covering broad organisational and social issues (Dhillon & Backhouse 2001; Straub et al., 2008). This study acknowledges these issues and provides a solid conceptual foundation for future studies on IS Security by answering calls for a theoretical model to guide research in the area.

S SECURITY CATEGORIES			
CATEGORIES	**%**	**CATEGORIES**	**%**
Legal aspects of IS Security	3.35 %	Computer crime	2.50 %
General IS Security	6.64 %	Database security	6.25 %
Business continuity planning	3.20 %	Intrusion detection systems	2.96 %
IS Security management and planning	8.83 %	Network and communication security	10.85 %
Operating System security	2.50 %	Secure systems design	2.57 %
Risk management	2.96 %	Identification and authentication	3.59 %
Viruses and malware	4.76 %	Cryptography	10.93 %
Security and privacy	2.18 %	Security behaviour	1.17 %
Copyright and piracy issues	1.32 %	Hackers and hacking	1.64 %
Security policies	1.25 %	Public key infrastructures	1.32 %
Computer forensics	2.26 %		

Table 1.1: IS Security Categories.

1.3.2 The Rigour of this Study

The criteria for conducting positivist assessments of research are objectivity, reliability, internal validity and external validity (Lincoln & Guba, 1985). However this criterion is not suitable, when judging the quality of qualitative research. An overview of the research design is illustrated in Table 1.2. In order to realise this exploratory study's research objective, an integrative conceptual model and a related research analysis framework are employed to investigate the relationship between IS Security and KM within two multinational organisations: CME-Co and TELE-Co. Two of the key strategic units within the cases are the IS Security and Customer Support (CS) functions which operate as silos servicing (in/external) customers. These case studies were selected from a population of large multinationals in two market sectors (storage and telecommunications) to facilitate (Drake et al., 1998) the study of the phenomenon in a diverse setting. The theoretical model (Section 2.7.1, p.59) draws on the KM and IS Security literatures from which three research questions are formulated (Section 1.3). These research questions are posited to guide the conduct of the study. In addressing these questions, the findings of the two case studies present a cross-case analysis of the different approaches to managing (IS Security) knowledge; these are then synthesised to determine comparisons, differences and impacts across the cases.

RESEARCH LEVEL	DETAILED DESCRIPTION
Type of Research Q	To explore how ISS could leverage the concept of KM through qualitative research
Strategy	Qualitative: Two case studies and a Pilot Case Study
Paradigm	Interpretivist
Data Collection Method	Semi-structured Interviews
Other Data Sources	Document Analysis, Observation
Major References	DeLone & McLean '03; Becerra-Fernandez et al., '04; Siponen, '05; Dhillon, '06
Informants	IT Professionals: ISS Experts, CS Engineers and Senior IS Managers
Type of Results	In-depth reflective descriptions and patterns of behaviour

Table 1.2: The Research Design.

The next section presents the organisation of this thesis.

1.4 Organisation of the Thesis

This thesis first examines the literature on IS Security (Figure 1.1). **Chapter 2** presents a critical analysis of the different strands of IS Security. The current security landscape is explored as is the importance of controlling IS Security to protect (knowledge) assets from known threats. The various controls and models necessary to protect an organisation and their implementation are also described. KM is then discussed as a possible approach to managing IS Security knowledge and as a conceptual model and research lens to this research is discussed.

Chapter 3 describes the research philosophy, epistemology, methodology and design. The appropriate methods of qualitative data collection, analysis and displays are outlined. The Chapter concludes with a description and illustration of the research protocol used in a series of six steps to explain how the study has been conducted.

Chapter 4 applies the research protocol developed and described in Chapter 3 to a pilot case study.

Chapters 5 and **6** provide the context to the study, to understand the environment in which the IS Security and CS functions under analysis operate. While the focus of the research is primarily the IS Security and Customer Support functions within each case, the rich description used allowed the researcher to describe the case studies systematically and identify the different research categories due to the use of the research lens identified in Chapter 2. An analysis of the contrasting goals, strategies and approaches to the management of knowledge between Customer Support and IS Security functions explained how the methods applied in one context can be transferred to the context of other functions with tangible benefits.

Chapter 7 conducts an integrative cross-case analysis of the findings. The analysis is structured by the conceptual model and associated research questions. The cross-case analysis provides a generic understanding of the relationship between IS Security and KM across the two case studies. This Chapter concludes with a summation of the overall findings which includes a refined theoretical model of an integrated approach to managing IS Security knowledge and an analysis of the interplay between KM and IS Security. Chapter 7 therefore provides an understanding of the phenomenon and allows explanation to give rise to understanding.

In **Chapter 8** existing literature and existing theories are discussed with the purpose of building internal validity and increasing the theoretical basis of the study's research findings. An integrated model for IS Security knowledge is presented as a practical approach for practitioners to manage IS Security for organisations and IS Security knowledge. This Chapter presents a critical review of the strengths and weakness of the interpretivist approach adopted and presents recommendations for future research.

The concluding section outlines the contribution of the empirical findings. It is clear from the analysis presented in Chapter 8 that this study provides a timely answer to calls in the IS field for in-depth exploratory research of a qualitative nature on the phenomenon of IS Security. Additionally, the overall goal of this research is to ensure that the findings are of value to practitioners and to do rigorous research in addressing the research questions and objective.

1.5 Conclusion

In this study qualitative research is used to explore how IS Security can leverage the concept of KM. The unit of analysis is the (ISS and CS) support function or specialised unit. This research adopts a case study approach, interviewing participants in two multinationals. Data was gathered in the form of interview transcripts and documents. A number of people in each organisation were interviewed (Table 3.3), providing a range of opinions and reports of practice. The use of semi-structured interviews provided a framework for identification of approaches to managing IS Security and CS knowledge, while allowing sufficient freedom for interviewees to report important data. This research extends current understanding of IS Security and of managing IS Security knowledge. Its findings provide a basis for an integrated model for managing IS Security knowledge. The following Chapters of this thesis are presented in diagrammatic form in Figure 1.1. The diagram depicts the flow through the Chapters, with the research objective arising from the relationship between IS Security and knowledge management, testing the conventional view of managing IS Security knowledge in a compliant environment.

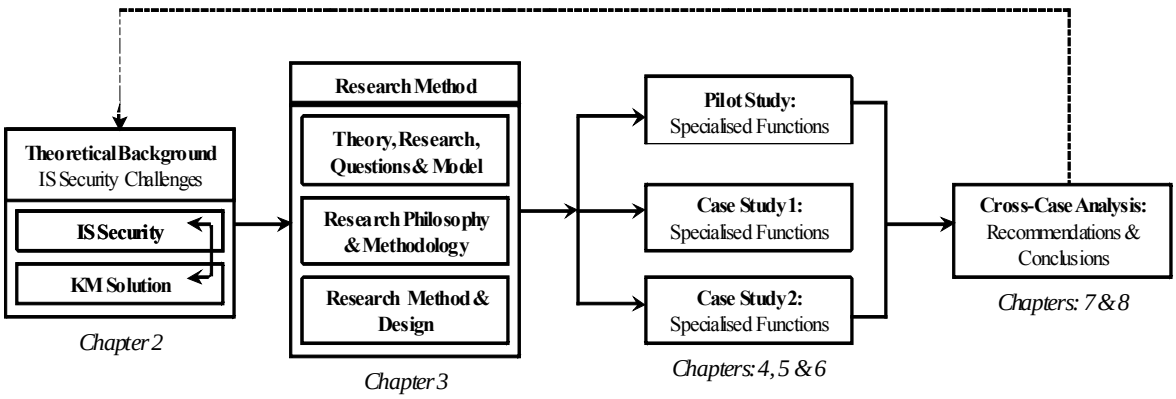

Figure 1.1: Plan of Research.

CHAPTER TWO

FRAMING THE IS SECURITY LITERATURE

2.0 Introduction

This Chapter first reviews the IS Security (ISS) literature examining the nature of ISS, and defining it for the purpose of this study. Section 2.1 describes the importance of using a framework to structure the literature and outlines the framework used in this Chapter. Section 2.2 examines the evolution of IS Security to become a strategic function within organisations. The section also defines IS Security and highlights its importance in the IS field. Section 2.3 establishes how IS Security is institutionalised and the different roles and responsibilities necessary to manage IS Security. Section 2.4 classifies the formal controls and models utilised in IS Security. Section 2.5 highlights the IS Security challenges encountered in organisations, and Section 2.6 discusses IS Security from a knowledge management perspective, describing the knowledge types, knowledge reservoirs and approaches used in KM. Section 2.7 explains that organisations need to apply an integrated approach to managing IS Security and a research lens is derived from this literature to investigate the objective of this study. Finally, Section 2.8 concludes the Chapter (Figure 1.1).

2.1 Framework for Analysis

One of the fundamental steps in reviewing literature is the selection of an appropriate framework to organise and analyse the (IS Security) literature (Webster & Watson, 2002; Siponen, 2005; Siponen & Willison, 2007). The purpose of this section is to identify existing frameworks in the IS Security literature and their effectiveness. This section also outlines the framework used in this Chapter to understand and summarise relevant IS Security and KM literature.

There are several frameworks which have been used to analyse Secure Information Systems (SIS) methods and approaches (Baskerville, 2004). Dhillon and Backhouse (2001) analysed IS Security methods in the context of the four sociological paradigms proposed by Burrell and Morgan (1979). Siponen (2005) selected research methods, the organisational role of IS, research objectives and applicability to ISD as his conceptual framework to analyse IS Security methods. While these approaches produced interesting findings, there were deficiencies (Siponen & Willison, 2007; Siponen et al., 2008). Each study investigated methods for secure IS, not the people, processes and technologies which embody IS Security functions. IS Security is a knowledge-intensive activity (Sundt, 2006) therefore the effectiveness of current approaches (originally created for developing information systems) to managing IS Security have been seriously questioned (Siponen, 2005). Technical approaches to IS Security have limited effectiveness as security is primarily a people issue. IS Security requires the development of an integrated approach to the management of IS Security knowledge. For the purpose of this study a framework was created. A number of different viewpoints were selected such as the: IS Security challenges facing practitioners, organisational role of IS Security, traditional IS Security methods, IS Security activities, technical counter-measures, IS Security knowledge, reservoirs of IS Security knowledge

and the use and impact of KM for this study. Table 2.1 outlines the framework for analysing the literature. It is theoretically important to adopt a framework to understand and summarise relevant IS Security research. However, to begin with, the evolution of IS Security is discussed (Section 2.2).

VIEWPOINTS	SOURCE REFERENCES
How did IS Security evolve?	Borodzicz, '05, Baskerville, 05; Siponen, 05
How is IS Security defined?	Baskerville & Siponen, 02; Anderson, 03
How is IS Security institutionalised?	Dhillon, 01; Dutta & McGowan, 02; Baskerville & Siponen, 02
What are the different activities?	Andress, 04; Whitman & Mattord, 05;Sundt, 06
What are the technical solutions?	Stewart, 05; Mishra & Dhillon, 08
What are the diff. methods & models?	Baskerville, 94; Dhillon & Backhouse, 01; Baskerville, 04
What is the IS Security challenge?	Baskerville, 04; Dhillon, 06; CSI/FBI, 06; Randeree, 06
What is IS Security knowledge?	Jamieson & Handzic, 04; Belsis et al., 05
Where is ISS knowledge located?	Drucker, 93; Becerra-Fernandez et al., 04; Randeree, 06
What are the different KM processes?	Holsapple & Singh, 04; Avital, 04; Holsapple & Joshi, 04

Table 2.1: Framework of the Literature Analysis.

2.2 Evolution of Information Systems Security

The purpose of this section is to examine how IS Security evolved to become a strategic function within organisations. IS Security is beset with reports of negative incidents in practice and calls for qualitative studies and integrated approaches to managing IS Security within organisations are numerous in the IS field. This section concludes with a working definition of IS Security.

Theoretically the IS Security field is in its infancy (Dhillon & Backhouse, 2001; Borodzicz, 2005; Belsis et al., 2005; Dhillon, 2006; Siponen & Willison, 2007) and it draws from an assortment of informing disciplines (Dhillon & Backhouse, 2001; Stewart, 2005; Dhillon, 2006) from computer science which provide the technological aspect, law the regulatory restraints and behavioural science and anthropology provide the human and cultural implications for effective IS Security. The IS Security research community itself arose from the mathematical and natural sciences (Gerber & Von Solms, 2005; Botha & Gaadingwe, 2006). As a result, attempts to produce a cohesive, all-encompassing and regulated profession are ill-founded (Borodzicz, 2005, p.67). Additionally the fundamental issue in defining and categorising IS Security is that it is intrinsically fuzzy and under-researched (Manunta, 2000; Anderson, 2003; Borodzicz, 2005, Baskerville, 2005; Dhillon, 2006). Some theorists hypothesise that IS Security is, in fact, risk management in practice (Borodzicz, 2005). However Lievesly (1995) posits that even the term is incorrect and that researchers and practitioners should be discussing and implementing a "risk engineering" strategy as opposed to a IS Security policy or strategy. Therefore the:

> "…Socratic problem "What is Security?" is under-estimated and under-researched. Different answers are given, which are of value at the tactical and specific level. There is general agreement and a surfeit of information on the physical and formal aspects of security. Standards, technical details and codes of practice are available… None of them appears to address the concept of security. We need to understand what do we mean by "security" before addressing the problem: How can we attain it?"
>
> (Manunta, 2000, p.7)

Manunta (2000) contends that security is the function of three components: an asset (A), a protector (P) and a threat (T). Security can therefore be expressed in any situation (Si) mathematically as: S = f (A, P, T) Si. This approach eliminates the complexity of understanding the concept of IS Security but the problem is compounded when applied in different environments (Baskerville, 1993; Wood, 1999; Baskerville & Siponen, 2002). The most complex conception of IS Security is provided by Post & Kingsbury (1991). They suggest that the term should not be defined, as the definition will fail to include the other areas of study that support it, but rather understood within a theoretical discourse, in terms of eight categories. Table 2.2 outlines the themes or categories which Post & Kingsbury (1991) use as a lens for understanding the field (Stewart, 2005). However Anderson (2003) challenges Post and Kingsbury's (1991) contention that IS Security should not be defined. Anderson (2003) calls for an exact definition as if you cannot define IS Security you cannot measure it and "…you cannot manage what you cannot measure" (Baskerville, 2008, p.2). As explained by Wiseman (1988) the advancement of a field of enquiry depends on giving priority to measurement as well as in defining it.

CATEGORIES OF IS SECURITY	
1.	Historically security knowledge is composed of facts generated through the growth and development of society. The best examples are the changes in legislation and the development of codes of practice.
2.	The psychological focus would be in the study and interpretations of individuals and groups regarding the definition of security. In addition to trying to catch a hacker an organisation should also try and understand why and how to prevent future breaches.
3.	Sociologically security is viewed as an aspect of human social behaviour, society and cultural groupings and through human organisations and institutions. As corporate security is viewed as primarily an organisation or institution issue, it is difficult to view these in isolation from the others.
4.	The functionalist category is used in terms of the application of security by security personnel who have clearly defined roles.
5.	Management is divided into five major functions: planning (the management function of setting security goals), organising (the structure through which the tasks or goals are carried out), command (essentially leadership and motivating employees to achieve the optimum return on investment), coordination of activities to facilitate collaborative efforts and controlling the process of regulating organisational activities to achieve set standards and goals.
6.	The normative category or theme defines security in relation to defining norms and standards and then protecting and enforcing them.
7.	However the structural category views security in terms of the organisation's components and the control of these units to ensure the interoperation of the entity.
8.	Descriptive allows multiple definitions of security. The definitions can be based on context, environment and utility.

Table 2.2: The Eight Categories (Source: Post & Kingsbury, 1991).

This study focuses on the development of an integrated approach to managing IS Security knowledge. However, given the significance of the evolution of ISS, it is imperative that the researcher next defines what is meant by IS Security in the context of this study.

IS Security definitions focus on specific uses. In "...an information society, security emphasizes the protection of information and not only the infrastructure" (Gerber et al., 2001, p.32). There are ISS goals: confidentiality, integrity and availability (Parker, 1981, 1998; ITSEC, 1991) which are cited regularly in the literature (Dhillon, 2006). To further complicate matters Holsapple & Joshi, (2000) add knowledge validity (accuracy, consistency and certainty) and knowledge utility (clarity, meaning, relevance and

importance) as additional characteristics or IS Security goals when securing knowledge. If an organisation can not ensure and assure these goals, then the value of the data/information / knowledge will be reduced or lost (Jamieson & Handzic, 2004). The ultimate objective of IS Security is the alignment of security to the requirements of the business (Baskerville & Siponen, 2002) and the environment in which it operates (Baskerville, 2004). Hong et al., (2003) contend that IS Security is open to many definitions. Table 2.3 highlights some of the most common definitions and it is apparent that while many definitions with varying viewpoints of ISS have been provided since its inception, none capture all of the characteristics of ISS. This is because ISS is evolving and for the purpose of this study the following is a working definition:

> *IS Security is a process that ensures the protection of information resources encompassing the people, processes and technologies used.*

Additionally it is important to note that IS Security is not absolute (Neuman, 1995; Anderson, 2003; Behara et al., 2005) as "a [system] which aims to be one hundred percent risk free will have a productivity of zero percent" (Jones & Ashenden, 2005, p.188) making the issue of determining the optimal level of IS Security vital (Manunta, 2000). This section has detailed how IS Security has evolved to become a mission-critical function and the issue of determining the optimal level and management of IS Security is vital. Prior to addressing this issue, it is imperative that the researcher identifies how IS Security is institutionalised and the roles and responsibilities necessary to control IS Security. Section 2.3 describes its institutionalisation and 2.3.1 its governance.

INFORMATION SYSTEMS SECURITY DEFINITIONS		
Definition	**Viewpoint**	**Authors**
"The process of controlling and securing information from inadvertent or malicious changes and deletions or unauthorized disclosure is IS Security".	Processes	URN 96/702, 1996, p.3
"…as all aspects related to achieving and maintaining confidentiality, integrity, availability, audit ability (accountability), authenticity and reliability".	Goals	ISO, IEC TR 13335-1, 1996, p.1
"…is not just about protecting the technology, it is about protecting business or personal information wherever it resides".	Technology	Willis, 1999, p.1
"Information systems security is not a contradiction in terms…security without risk management is".	Risk management	Bisson, 2003 in BS7799, p.3
"… the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats".	Access to objects	U.S. National Information Systems Security Glossary
"…as to apply any technical methods and managerial processes on the information resources (hardware, software, and data) in order to keep organisational assets and personal privacy protected".	Protection	Hong et al., 2003, p.243

Table 2.3: Definitions of IS Security (ISS).

2.3 Institutionalising Information Systems Security

The purpose of this section is to describe the complexity of securing organisations and to discuss the roles and responsibilities necessary to protect them. Responsibility is the foundation of IS Security governance in defining the control structure for the organisation. Sections 2.3.1 and 2.3.2 provide an overview of the roles of senior management and ISS functions in managing ISS. This section concludes with a description of the culture and informal controls necessary to create the correct control environment necessary to preserve and govern the security of the organisation.

Societies and organisations increasingly rely on computers and global networks such as the Internet to carry out their business communications, transactions, and supervision of employees. Emergent organisational forms endure continual change and are difficult to secure (Baskerville, 2004; Dhillon, 2006). As organisations grow in size and complexity information handling becomes increasingly difficult and important. Information communication technologies (ICT) have enabled large, complex and global organisations to be competitive and adapt to changes in their environment (Truex & Baskerville, 1998; Baskerville, 2004). Emergent organisations are then unstable and often unresponsive to centralised control which can be problematic from an IS Security perspective. Due to the sheer complexity of modern organisations, security failures and the implementation of continuity plans are common (Reason, 1997; Borodzicz, 2005). IS Security convergence, a trend affecting global enterprise is the identification of security risks and interdependencies between business functions and processes (Booz et al., 2005). Security convergence is pushing companies to focus beyond functional dimensions to include all parts of the security and the business life-cycle in creating a need for a unified security environment.

A further layer of complexity is added when organisations establish relationships with other enterprises (Gal-or & Ghose, 2005; Dhillon, 2006). IS Security managers will need to manage increasingly complex security architectures in support of emergent organisations. These are composed of a series of information handling activities (Stamper, 1973) coordinated through the establishment of rules, policies and procedures (Baskerville & Siponen, 2002; Dhillon, 2006). As organisations grow, controlling information by assuring its integrity and availability can be extremely difficult. Organisations must design and create a safe environment in which business processes, procedures, employees and units can function. This environment must maintain the confidentiality, availability and integrity of the organisation's information/knowledge (Doyle, 1997; Jamieson & Handzic, 2004).These goals are met through the application of an IS Security strategy or policy. Information and knowledge are undoubtedly critical resources of the enterprise (Escamilla, 1998). However these are becoming increasingly endangered by security threats (Whitman, 2004; Eschelbeck, 2005; Im & Baskerville, 2005; CSI/FBI, 2006). In order to implement a successful security management strategy, management needs to develop an underlying IS Security model to protect knowledge assets, operationalise risk assessment and create an effective control environment (Dutta & McCrohan, 2002). This environment enables organisations to keep to their overall plans, as they move from their IS Security objectives to their IS Security outcomes.

Methods, strategies and procedures ensure the protection of an organisation's resources and adherence to IS Security standards (such as ISO17799). Therefore an enterprise-wide IS Security policy can function as a guide in determining the corporation's weakest links (Baskerville & Siponen, 2002). These will then be the basis for

formulating policies or strategies and procedures for risk and IS Security management (Booz et al., 2005; Jones & Ashenden, 2005). Matrix structures can cause more complicated process flows compared to hierarchical structures (Borchgrave et al., 2001). Therefore the role of senior management is to guarantee that its structure is supportive of the exploitation of IS Security-related initiatives, without necessarily impeding business processes. Borchgrave et al., (2001) warn that separating particularly sensitive processes into peculiar structural entities will require the development of additional IS Security measures specifically for the new entities (such as geographically dispersed subsidiaries). Another implication is the modification of communication lines, reporting relationships or accountability to attain IS Security strategies and objectives. Dhillon (2006) further stresses the importance of the culture and structure of the organisation as he extrapolates that IS Security of information at a structural level is largely related to linking access rights to the hierarchical structure of the organisation.

2.3.1 Responsibility and Corporate Governance

It is the responsibility of senior and IT management to protect the organisation's ability to function (Cresson Wood, 2001; Dhillon, 2005; 2006). Structures strongly influence primary corporate activities engagement. Dutta and McCrohan (2002) suggest that if there is an absence of a group or unit responsible for IS Security activities then IS Security may become a futile function. Therefore structure adds capability to match corporate objectives by supplying a complete framework for planning and developing an organisation. The assignment of authority and responsibility is an extension of the development of structure.

Figure 2.1 illustrates a generic responsibility model for the average organisation and demonstrates how challenges or issues related to IS Security management affect different responsibilities (Dhillon, 2005). The relationship between (corporate) governance and IS Security exists in a number of different forms (Dhillon, 2006). The corporation is responsible to its creditors, stakeholders and for legal requirements. However corporate officers are responsible for IS Security through the application of formal (policies, procedures and audits), technical (compliance, access lists and audits) and informal (ethics and behaviours) controls. Corporate officers can demonstrate responsible behaviour and meet compliant requirements (Kaen, 2003) through corporate governance. Corporate governance is concerned with who has legal control (Kaen, 2003; Borodzicz, 2005) which creates challenges for management. The scandals of Enron and Barings Bank were significant drivers for more regulations. IT and IS Security were impacted by the Sarbanes-and-Oxley (SOX) Act (2002) which grounds the call for better business and IT controls in legislation. The primary goal of the Act is to produce more complete and accurate financial reports and over eighty billion dollars has been reportedly spent between 2005 and 2006 on regulatory and compliance-based work (Chou, 2005).

Barings Bank and Enron are cases of mismanagement of IS Security (Dhillon, 2006). Barings Bank was brought down by weak IS Security which allowed an employee to hide losses accumulated in a secret account he created with his "access rights to the bank's accounting systems" (Dhillon, 2001; Haworth & Pietron, 2006). Enron has had ramifications for American overseas subsidiaries. Regulators alleged that this type of fraud and corruption was possible because of loopholes in U.S. securities laws and poor auditing controls, resulting in inflated profit margins. It is through IS Security that tighter access controls for the environment are assigned. Additionally, the allocation of senior responsibility through corporate governance has increased corporate security

awareness (Kaarst-Brown & Kelly, 2005; CSI/FBI, 2006). Corporate governance defines the control structure and control of tangible and intangible information assets and corporate knowledge. Corporate governance emphasises accountability, fiduciary duty and methods of auditing and control (Sundt, 2006).

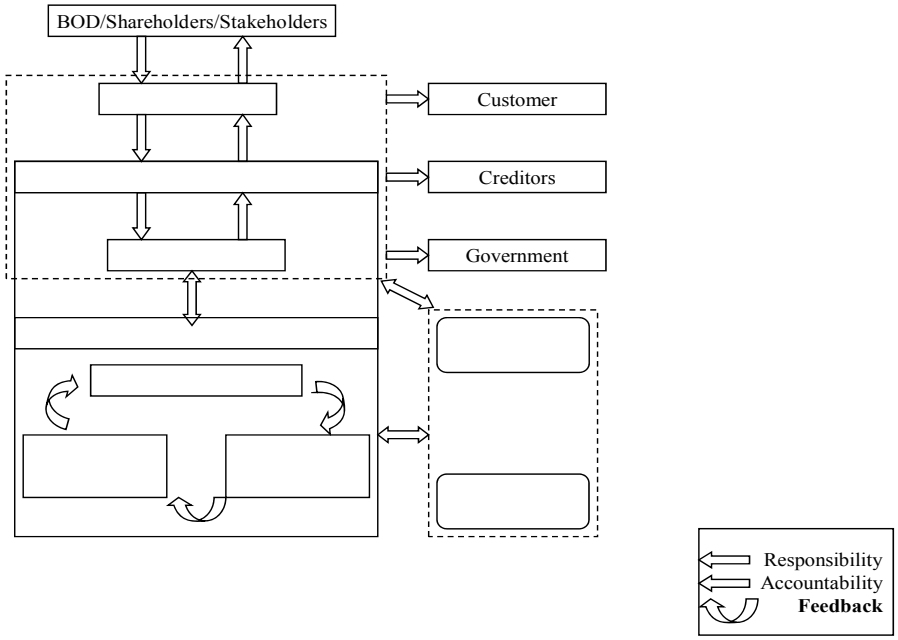

Figure 2.1: Model of Responsibility & Corporate Governance for IS Security (Source: Dhillon, 2005, p.214).

Trompeter and Eloff (2001) argue that organisations should use confidentiality, integrity and availability (C.I.A) standards and security services to govern IS Security. To achieve C.I.A internally organisations should adopt ethical principles. The organisation would engender IS Security and ethical awareness in adhering to regulatory requirements and protect information assets. Smith and Hasnas (1999) contend that the adoption of a code of ethics can have significant consequences (Reynolds, 2003; Whitman, 2004). Customers and society are often affected by the decisions of corporate decision-makers (Dhillon, 2006). That is IS Security managers must choose between competing ethical stances (Smith & Hasnas, 1999). Failures in governance have been due to a lack of awareness and conflicts of interest. There is a documented failure of management in recognising the extent to which IS Security is critical (Dhillon, 2006) and ethical issues regarding security and privacy can have far reaching consequences. As a result there is a fundamental requirement for the governance of IS Security. Moulton and Coles (2003) refer to security governance in terms of: IS Security responsibility and practices, strategies and objectives for security, risk assessment and management, resource management for security, compliance with legislation, regulations, security policies and rules, investor relations and communication activities in relation to security. Ultimately it is the responsibility of management to align security activities with the goals of the organisation (IT Governance Institute, 2001). Therefore IS Security must be mapped to every business function and process (Patterson, 2005).

2.3.2 Information Systems Security Management

Comparatively little research covers organisational and social issues regarding IS Security (Dhillon & Backhouse, 2001; Straub et al., 2008). Senior management and the Chief Information Officer (CIO) must set policies and ensure that the organisation is compliant with the complex and often shifting legislation that controls Finance and the use of IT. Management often digress from decisions regarding IS Security as they regard it as a technological issue and the responsibility of IT (Dutta & McCrohan, 2002; Hinde, 2002). However as Wood (2001, p.1) stated "…IS Security is a management issue in addition to a technical issue, it is a people issue in addition to the technical issue". As described by Andress (2004) the role of management within IS Security is to identify crucial (knowledge) assets, initiate a process of risk management and maintain a general operational balance within the organisation to assure productivity (Jamieson & Handzic, 2004).

Organisational structures strongly influence the implementation of IS Security activities and the consistency with which they facilitate the enterprise's goals. For example if there is an absence of an individual or section that is solely accountable for IS Security issues (such as a IS Security function) then the deployment of activities related to security may be slow, hampered or futile (Dutta & McCrohan, 2002). The role of senior management is to guarantee that its structure is supportive of the deployment of security-related initiatives, without necessarily impeding business processes. This may indicate separating particularly sensitive processes into different structural entities and establishing more security measures specifically for them. Another implication is the modification of communication lines, reporting relationships or accountability to attain security strategies and objectives (Borchgrave et al., 2001). Von Solms and Von Solms (2004) highlighted a number of mistakes commonly made by management regarding IS Security (Table 2.4). The role of management is vital in assuring conformity to environmental drivers such as compliance regulations and the development of effective IS Security policies (Baskerville & Siponen, 2002). However these requirements are often enforced by an IS Security function.

TEN DEADLY SINS OF IS SECURITY MANAGEMENT	
1.	Not realising that IS Security is a corporate governance responsibility
2.	Not realising that IS Security is a business issue not a technical issue
3.	Not realising the fact that IS Security governance is a multidimensional discipline
4.	Not realising that an IS Security plan must be based on identified risks
5.	Not realising the importance of the role of international best practices
6.	Not realising that IS Security policy is absolutely essential
7.	Not realising that IS Security compliance enforcement and monitoring is absolutely essential
8.	Not realising that a proper IS Security governance structure is absolutely essential
9.	Not realising the core importance of IS Security awareness among users
10	Not empowering IS Security managers with the infrastructure, tools and supporting mechanisms to perform their responsibilities properly

Table 2.4: Ten Deadly Sins of IS Security Management (Source: Von Solms & Von Solms, 2004, p.372).

2.3.3 The Information Systems Security Function

Dutta and McCrohan (2002, p.84) contend "…that only senior management can initiate the plans and policies that address the different aspects of security in a balanced and integrated manner". They further state that leaving the aspect of IS Security in the hands of the IT department "…will strengthen …technology and will not yield intended results. IS Security lapses are management failures more than technical failures". The study of people and groups/units can be traced back to as early as the 19th century. For example, Gustave LeBon (1896) investigated the absorption of individuals into a crowd, losing their personality and adopting the collective mind of the group, such as a departmental group. The role that groups come to play in their organisation cannot easily be tied down to simple models (McGrath, 1984). Organisations and functional areas evolve and the result is rarely a neat arrangement of groups and procedures (Brown & Magill, 1994; Strassman, 1995). A wide range of employees is required to support a diverse IS Security plan. The individuals responsible for IS Security are vital in ensuring the success of any plan to prevent known threats and respond to unplanned incidents (Im & Baskerville, 2005). IS Security also depends on the utilisation of external professionals such as communities of practice (CoP). These communities are composed of a group of individuals united by similar interest/values (Wenger & Snyder, 2000). People are the missing link to improving IS Security. Therefore, a specialised IS Security function is fundamental in assuring corporate assets.

The management of IS Security is a significant challenge due primarily to the increase in value of information (Behara et al., 2007) and knowledge (Jamieson & Handzic, 2004; Randeree, 2006). Due to the nature of IS Security issues organisations utilise a number of analytical tools to aid decision-makers to enact the functions of IS Security with their allotted resources. Given the high cost of IS Security it is necessary to determine the most effective approach and level of investment. The most practical or common approaches include: Cost based analysis (CBA), Net Present Value (NPV), Internal Rate of Return (IRR) (Gorden et al., 2006) and risk management, all of which focus on the financial or managerial evaluation of IS Security investments (Behara et al., 2007). As explained by the CSI/FBI 2006/07 surveys the majority of the respondents conduct some form of economic evaluation of their IS Security expenditures, with forty-two percent using ROI, twenty-one percent using IRR and nineteen percent NPV. The survey also identified economic and management issues (for example risk management) as among the most critical issues. However the overall objective for any organisation is to identify and strive toward the optimal level between IS Security and insecurity. The level is reached when the cost of additional IS Security countermeasures exactly equals the resulting reduction in damages arising from security breaches (Marin, 1992). Organisations must therefore determine the affect of too little or too much IS Security. Insufficient IS Security might leave the organisation vulnerable to attacks and ultimately reduce the corporate profit margin, and too much IS Security would mean that the high costs of IS Security countermeasures would consume profits (Bjorck, 1996) and reduce productivity (Jones & Anderson, 2004).

Security countermeasures have other consequences; there are social, legal and ethical issues. To further complicate the issue of determining the optimal level of IS Security, the most valuable asset an organisation has is often intangible, such as information and knowledge assets which are difficult to assess (Jamieson & Handzic, 2004, Booz et al., 2005; Holsapple & Singh, 2005). The technical control solutions, properly implemented, can improve an organisation's ability to balance the objectives of making information more readily and widely available against increasing the information levels

of confidentiality and integrity (Whitman & Mattord, 2005; Dhillon, 2006). Therefore while the need for, and management of, IS Security is justified, to succeed within the environment, people, processes and technology involved must be understood and implemented into the organisation. The next section describes the importance of organisational culture for IS Security.

2.3.4 Organisational Culture

Culture is an elusive concept with numerous researchers linking culture to enhanced coordination and control, improved goal alignment and increased employee effort (Gordon & DiTomaso, 1992; Dojkovski et al., 2007). De Long and Fahey (2000) contend that culture includes more explicit artefacts such as norms and practices, symbols, as well as language, ideology, rituals and myths (Pettigrew, 1979). Jermier et al., (1991) distinguished between tacit and explicit components of culture, describing the tacit aspect (assumptions) as ideational while the more explicit artefacts of culture (norms and practices) are referred to as material. Schein's (1985a, 1985b) three leveled model of culture describes both the more observable aspects of culture and the less observable aspects. As described by Schein (1985a) basic assumptions are at the core of culture and represent the belief systems that individuals have toward human behaviour, relationships and truth. These basic assumptions are formed over time as members of a group or function develop strategies to cope with solving problems and share these techniques and solutions with new members (or other practitioners). At the next level, corporate values form the foundation of corporate culture and provide a basis for appropriate behaviour (Deal & Kennedy, 1982). Schein (1985a, 1985b) makes it clear that values are merely a reflection of the underlying cultural assumptions. At the third level, culture is manifested through visible artefacts (for example heroes, language and rituals).

However, artefacts, such as information technology, are not culturally neutral and may come to symbolize a number of different values driven by underlying assumptions and their meaning, use, and consequences (Leidner & Kayworth, 2006). Schein (1985b) argues that values are more easily studied than basic assumptions, which are invisible and therefore not easily studied, as well as cultural artefacts (technology) that, while visible, are not easily decipherable. Therefore it is understandable that the vast majority of theories that conceptualize culture do so in terms of reference group value orientations (Jackson 1995) such as value dimensions at the organisational and functional levels. These have an impact on subsequent behaviours of firm members through acting as a means of social control that sets the expectations and boundaries of appropriate behaviours for members. Thus, the study of organisational values may be particularly useful in explaining certain behaviours with respect to how social groups interact with, for example, applying IT in organisational contexts (Leidner & Kayworth, 2006).

2.3.4.1 Cultural Topologies

Cultural theory argues that one's social position can be defined by two basic dimensions *grid and group*, subsequently producing four ways of life, each with a corresponding bias. *Group* refers to the extent to which an individual's freedom is controlled by the group in which they live or work (Jackson & Philip, 2010). Douglas (1970) recognises that belonging to group can place constraints on how people behave. In a high group environment, workers will be compelled to act in accordance with the collective interests of the group. In low group environments, members will be less compelled to

act in the interests of the group, and are free to associate and interact with other groups and individuals. In the group dimension, individuals have a choice as to whether they want to belong to a group. The application of these two dimensions: *grid and group* result in four approaches to life with contrasting cultural cosmologies (values and beliefs of a way of life) (Douglas, 1970). These include and are summarised by Jackson and Philip (2010):

(1) *Fatalism* is characterised by strong grid and weak group. Individuals exemplifying this way of life display values of apathy and fear. This creates a hampering environment to transcend throughout the organisation in times of change (Kaarst-Brown & Robey, 1999). It possesses no enabling characteristics.

(2) *Hierarchism* is characterised by strong grid and strong group. There will be a strong emphasis on order, discipline and coordination of tasks. It provides visionary leadership and coordination. However, too much control and power can smother vision, foster dissatisfaction and lead to an impassive cultural orientation (Tolsby, 1998).

(3) *Individualism/Market* is characterised by both weak grid and weak group. There will be opportunities for creativity and innovation. In its constraining form it can create a culture where individuals seize opportunities to their own advantage, leading to non-collaborative behaviour (Tsohou et al., 2006).

(4) *Egalitarianism* is characterised by weak grid and strong group. Group concerns take priority over individual interests. Members will stress the importance of group-ethos, teamwork and trust. In its enabling form, egalitarianism fosters knowledge sharing, teamwork and trust to exist between organisational members (Adler, 1991). Change can only be effective if individuals are willing to work as part of a team or a function/group. In its constraining form, egalitarianism due to its lack of leadership and authoritative values, can lead to breach of trust and unsettled disagreement and internal rivalry.

Therefore, according to Jackson and Philip (2010), managers should strive to reduce the constraining cultural characteristics and create a facilitative socio-technical environment by promoting the enabling cultural values. Organisations and functions, such as support, require the drive and innovation of *individualism/market* for enhancement and improvisation; the visionary leadership, resources and coordination of *hierarchism*, and the teamwork, trust and knowledge sharing of *egalitarianism*. This view is supported by a number of researchers (Ruppel & Harrington, 2001; Hendriks, 1999; Adler, 1991). However, membership of a cosmology is not fixed or permanent. It is dynamic as an individual could be a member of multiple cosmologies at the same time and drift between them forming, for example, technical communities of practice (CoP) in fields such as IS Security.

2.3.4.2 IS Security Culture

IS Security culture is composed of more than the confidentiality, integrity and availability of messages (Dhillon, 2006). Policies and procedures which are clearly articulated and supported by management are a good mechanism for setting the cultural tone regarding risks (Greenstein & Feinman, 2000). Beliefs and best practices influence the behaviour of employees regarding IS Security (Thomson & Von Solms, 1998; Hu et al., 2008) and as a result staff should be aware of procedures aimed at preserving IS

Security of corporate assets. It is vital that IS Security awareness is instilled in the culture of an organisation (Ettinger, 1993) by the IS Security function and management (Borodzicz, 2005). Cultural differences can, however, create difficulty in determining what is and is not ethical. Difficulties arise when one nationality's ethical behaviour conflicts with the ethics of another national group, which is an issue for multinationals. Dojkovski et al., (2007) contend that the local organisation/subsidiary culture will affect the IS Security culture, as an open culture promotes a relaxed attitude in the ISS approach adopted. The key to leveling ethical perceptions within a small population is education and awareness (SETA). Therefore employees must be trained in expected behaviours of an ethical employee, especially in areas of IS Security, to ensure proper use of information systems. Deterrence is the best method for preventing illegal or unethical activity. Laws, policies, and technical controls are all examples of deterrents. Additionally tools such as E-learning, training and education are valuable in developing IS Security cultures (Siponen, 2000). Knowledge sharing and collaboration have also been found to increase learning at individual and organisational levels in order to develop an awareness and culture of IS Security (Dojkovski et al., 2007).

Pabrai (2005) contends that organisations, which lack security education and training awareness (SETA) procedures, are more vulnerable to accidental or intentional compromise of sensitive information. He further states that appropriate training and regular updates on business policies and procedures should be given to all employees and third-party users who manage sensitive information. Cheswick et al., (2003) argue that organisations should implement these procedures regularly as the organisation's IS Security needs change. An efficient SETA strategy will educate employees about vulnerabilities, security measures and the importance of sensitive information. Businesses must communicate information regarding IS Security policies, legal responsibilities and business controls to the workforce. Finally, education amalgamates the IS Security capabilities of the organisation into a collective body of information and aims to equip IS Security professionals with the ability for vision and positive response. A corporate code of ethics and culture can be introduced and developed during training, which will aid organisational security (Stevens & Brownell, 2000). The development of a secure organisation requires a collaborative organisational endeavour (Dutta & McCrohan, 2002). Further awareness measures should be persuasive (Siponen, 2000) and assessed regularly (Dojkovski et al., 2007). It is through the provision of an effective organisational ISS culture and awareness programme that employees will intuitively protect corporate assets (Dojkovski et al., 2007) despite threat from the environment.

Organisations are constantly reinventing themselves to cope with the challenges of their business environments (Baskerville, 2004) and threats (Vroom & Von Solms, 2004). Essentially, the organisational context can offer criminal opportunities due to a complacency towards IS Security, erroneous perception of risks, a technical perspective of IS Security risks, funding of IS Security, implementation of inappropriate controls and an inability to learn from, and utilise, compliance reviews (Willison & Backhouse, 2006). The correct control environment utilises documentation and guidelines such as IS Security policies which are crucial to an IS Security function's ability to sustain, preserve and govern the IS Security of the organisation (Im & Baskerville, 2005). Thus, Section 2.4 examines the underlying threats to an organisation and the importance of allocating the necessary controls to combat their negative effects.

2.4 Formal Aspects of Information Systems Security

The purpose of this section is to present the formal aspects of IS Security. Issues related to managing risks (Section 2.4.1), knowledge regarding the threats and challenges (Section 2.4.2) facing organisations and technical countermeasures (Section 2.4.3) are also outlined. Section 2.4.4 describes the regulations and standards affecting the management of IS Security. This section concludes with an overview of the formal models presented in the literature and highlights the inappropriate use of these models in managing IS Security (Section 2.4.5).

2.4.1 Managing Risk

This section highlights the importance of risk management as a vital activity in IS Security. It involves identifying, assessing and evaluating the level of risk facing the organisation in question (Borodzicz, 2006). Risk management involves the identification of known threats (Williams et al., 1995) and the process of risk engineering (Lievesly, 1995). The IS Security function must understand its internal and external environment and the company's relationship with IS Security before an effective IS Security solution can be coined. The process involves implementing effective control measures (formal, informal and technical) to maintain the optimum level of IS Security (Dhillon, 2006). This acceptable level is achieved through the introduction of a number of processes from risk and feasibility analyses to the evaluation of IS Security controls. Enterprises face enormous challenges in exposures to risks – be they IS Security or otherwise. However senior management and many IT executives lack sufficient knowledge and data about their own vulnerabilities (Im & Baskerville, 2005) and the potential cost of failure due to an inability to manage knowledge pertaining to IS Security (Belsis et al., 2005; Wiant, 2005; Willison & Backhouse, 2006).

IS Security function's and practitioner's knowledge of local threats, which form part of such risks, is often fragmented. Researchers have addressed the extent to which IS Security managers are cognisant of the nature of systems risk (Willison & Backhouse, 2006). This risk can be managed or reduced when managers are aware of the different threats and implement the most effective controls (Straub & Welke, 1998). Aken (1978) posits that a control is the use of interventions by a controller (Security Officer/Coordinator) to promote a preferred behaviour for the organisation in preventing threats. The following sections will examine the threats and challenges facing IS Security functions in order to identify their negative effects and the controls necessary to limit the cost incurred.

2.4.2 Threats and Challenges

A threat is the possibility of an action, or event which could infringe IS Security causing harm by exploiting the vulnerabilities of an organisation. The weakest point in IS Security is considered to be the organisation's greatest vulnerability. In the IS Security field this is referred to as the "principle of easiest penetration" (Parker, 1991; Dhillon, 2006). Knowledge of threats and attacks are crucial to management when allocating resources, formulating IS Security policies and performing risk assessments (Straub & Welke, 1998; Jones & Ashenden, 2005). Attacks can temporarily deny network resources and use them as a stepping-stone in attacking another organisation a strategy frequently used in critical infrastructure attacks (Gal-or & Ghose, 2005).

Table 2.5 outlines twelve categories of threats that an organisation's people, information and systems face (Whitman, 2003). The majority of threats can be prevented with controls or IS Security measures such as verification of commands through authentication techniques. Deliberate acts of espionage represent a broad category of electronic and human activities that breach the confidentiality of information. Controls such as firewalls (Section 2.4.3) are sometimes implemented to mark the boundaries of an organisation's virtual territory. These boundaries give notice to trespassers that they are encroaching on the organisation's cyberspace.

	CATEGORIES OF THREAT	EXAMPLES
1.	Acts of human error or failure	Employee mistakes
2.	Compromises to intellectual property	Piracy, copyright infringement
3.	Deliberate acts of espionage or trespass	Unauthorised access/data collection
4.	Deliberate acts of information extortion	Blackmail or information disclosure
5.	Deliberate acts of sabotage or vandalism	Destruction of systems or information
6.	Deliberate acts of theft	Illegal confiscation of equipment
7.	Deliberate software attacks	Viruses, denial of service (DoS)
8.	Forces of nature	Flood, fire
9.	Deviations in quality of service	Power and network connections
10.	Technical hardware failures or errors	Equipment failure
11.	Technical software failures or errors	Bugs, code problems, loopholes
12.	Technical obsolescence	Outdated technologies

Table 2.5: Threats to IS Security (Source: Whitman & Mattord, 2005, p.39, Adapted from ACM, Inc.).

To tackle the threat of worms and viruses IS Security functions need to keep their skills and knowledge current (Im & Baskerville, 2005). Additionally organisations and IS Security practitioners are required to understand any and all legal and ethical responsibilities to minimise financial penalties and reduce risks from the threats discussed (Sundt, 2006). Section 2.4.3 presents an overview of the different technical controls available and Section 2.4.4 examines the regulatory aspects of IS Security. Various standards and best practices are also discussed.

2.4.3 Technical Information Systems Security Countermeasures

The technical side of IS Security is a part of, but not the answer to, the different IS Security challenges. This section explores IS Security technologies, methods and models. Knowledge and expertise of the technologies necessary to alleviate IS Security risks are seen as valuable (Dutta & McCrohan, 2002; Belsis et al., 2005; Stewart, 2005). Technology is used by organisations to gather and share information while simultaneously protecting it. Therefore "…senior managers must be familiar with some of the critical components of security technology" (Dutta & McCrohan, 2002, p.74). Technological changes, in both secure hardware and software, are as constant as the increase in the number of threats to corporate IS Security. Secure protocols, standards and encryption are used to protect business environments (Stallings, 2001; Dhillon, 2006) and IS Security technologies such as firewalls, scanning tools and intrusion detection systems are used to filter out possible threats (Jamieson, 1991). Theoretically the data derived from these tools should, if utilised correctly, provide an integrated view or knowledge pertaining to the IS Security landscape of the organisation (Belsis et al., 2005; Booz et al., 2005).

Figure 2.2 illustrates a combination of the sphere of IS Security (Whitman & Mattord, 2005) and ISS controls aligned to corporate assets such as: data, information and knowledge. Each asset is mutually interdependent and of value requiring appropriate countermeasures. They are always at risk from attacks through the people and computer systems that have direct access to them. The sphere illustrates that between each layer there must exist a layer of protection in the form of countermeasures to prevent access to the inner layer from the outer layer. Technical controls are implemented between systems and the three assets, between networks and the systems, and between the Internet and internal networks. As illustrated, a variety of controls can be used to protect the data, information and knowledge stored by an organisation.

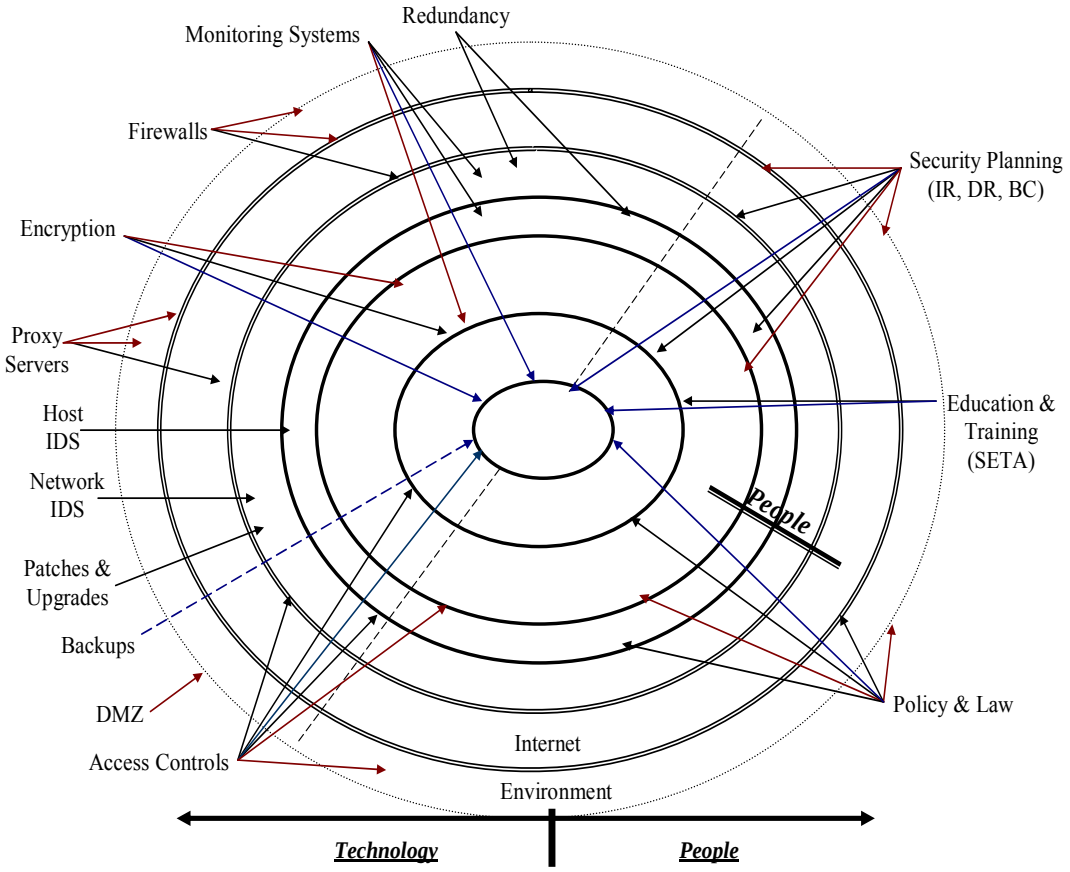

Figure 2.2: Proposed Countermeasures for data, information and knowledge (Adapted by the Researcher from Whitman & Mattord, 2005, p.198, Appendix A).

However, as people can directly access each ring as well as the knowledge at the core of the model, people require unique approaches to IS Security. Members of the organisation must become a safeguard, which is effectively trained, implemented, and maintained, or else they, too, become a threat to the information and knowledge stored. The most common counter measure is the firewall. Firewalls are often regarded as the first line of defence of an IS Security strategy (Andress, 2004). The most effective firewalls are able to optimise functionality, decreasing risk and cost efficiency. Intrusion detection systems (IDS) monitor both inbound and outbound activities of the network and computer systems for signs of IS Security violations (Escamilla, 1998). Having detected such signs, the IDSs trigger alerts to categorise and report them. The report is downloaded by an analyst who evaluates and initiates an adequate response (Whitman & Mattord, 2005). In practice IDSs can trigger thousands of reports per day of which

the majority are false positives (benign events) making it extremely difficult for the analyst to filter and identify true positives (attacks).

Access controls permit or deny the use of an object (a passive entity, such as a system or file) by a subject (an active entity, such as an individual or process). Access control systems provide the essential services of identification and authentication, authorisation, and accountability where identification and authentication determine who can logon to a system, authorisation determines what an authenticated user can do, and accountability identifies what a user did (Andress, 2003; Cheswick, 2003; Dhillon, 2006). Strong (layered) authentication is often coupled with high investments in the security infrastructure (Cheswick et al., 2003; Andress, 2004). Cryptography is the use of mathematic formulas to encrypt and decrypt data allowing individuals to store sensitive information or transmit it across insecure networks (Stallings, 2001; Sundt, 2006). It is extremely important for data security and e-commerce in addressing confidentiality, authentication, integrity and non-repudiation (Whitman & Mattord, 2004). Virtual private networks (VPNs) utilise encryption when establishing connections over an existing shared infrastructure using encryption or authentication technologies to secure its information. Virus scanners function by constantly screening all inbound network traffic. This technology is used by nearly ninety-six percent of organisations (CSI/FBI, 2005).

The same technologies which have empowered global commerce are also empowering hackers and hacking organisations to subjugate different types of information systems (Baskerville, 2004; Stewart, 2005). Advanced firewalls and virtual private networks (VPN) can be used (unintentionally) to fragment organisational information systems into IS Security compartments (Baskerville, 2004; Dhillon, 2006) making them difficult to monitor and control. There has been a consolidation of larger vendors but the market does remain fragmented with specialised vendors in for example IDS. The IS Security market is essentially vendor driven in which IS Security capabilities (products) are widely available for any business to purchase. Gartner estimates that worldwide IS Security software revenue totalled seven and a half billion dollars in 2005 (CSI/FBI, 2007). It is common practice (for vendors) to manipulate internal taxonomies of vulnerabilities to make vendor figures look more impressive, creating a false perception of value (Stewart, 2005). Vendors in the IS Security space have a vested interest in playing up the perception that organisations face rapidly increasing threats/risks, and management should approach their claims with appropriate scepticism (CSI/FBI, 2007). As IS Security breaks out of its technical citadel to become a ubiquitous reality for all users of information, there is a pressing need for a theoretical framework against which practitioners may diagnose problems, plan action and implement solutions (Willison & Backhouse, 2006).

The next section describes IS Security regulatory drivers.

2.4.4 Information Systems Security Regulations

An elementary part of the IS Security function's responsibility is a careful examination of current regulations and common ethical expectations of national and international entities. Laws and regulations increasingly affect how IS Security is implemented. This analysis provides insight into regulatory constraints that govern business (Sundt, 2006). Therefore this section examines key laws that shape the field of IS Security.

The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999 requires all financial institutions to disclose their privacy policies on the sharing of non-public personal information. The act ensures that the privacy policies in effect in an organisation are fully disclosed when a customer initiates a business relationship. However it is the compliance to the Sarbanes-and-Oxley Act of 2002 that has had a profound effect on IS Security and IT as well as Finance and legal departments (Kaarst-Brown & Kelly, 2005; Dhillon, 2006). Therefore IS Security practitioners require a wide range of skills far beyond technical computer security but which encompasses business, legal awareness and organisational process knowledge (Sundt, 2006). The SOX Act primarily addresses financial reporting and accounting controls; however it has inadvertently had a significant operational impact on IS Security management. Dhillon (2006) contends that IT and IS Security can be leveraged by an organisation in order to comply with the requirements of the law (Kaarst-Brown & Kelly, 2005).

Figure 2.3 illustrates and outlines the impact of SOX on IS Security. The initial and most obvious impact has been the creation of a new reporting structure which must be implemented by IT/IS Security functions. IS Security will have to assure authentication of data through the use of technical controls. Specialised IS Security structures or functions must document in detail the logging of data access and/or modifications, control structures and processes. Adequate storage and back-ups of relevant corporate data assets (emails, audits, and financial reports) must be provided and implemented. Legal liability may arise from the use of, for example, a knowledgebase (Zeide & Liebowitz, 1987; Jamieson & Handzic, 2004) therefore it is the responsibility of the IS Security function to assure compliance to relevant laws. The Sarbanes-and-Oxley legislation has created a greater need for businesses to implement IS Security controls to enforce "separation of duties[1]" and therefore controlled access to information. The greatest challenge, especially in organisations with complex structures and incongruent financial processes, is to construct testable, consistent, transparent, and complete auditing processes to determine the level of compliance (Sundt, 2006).

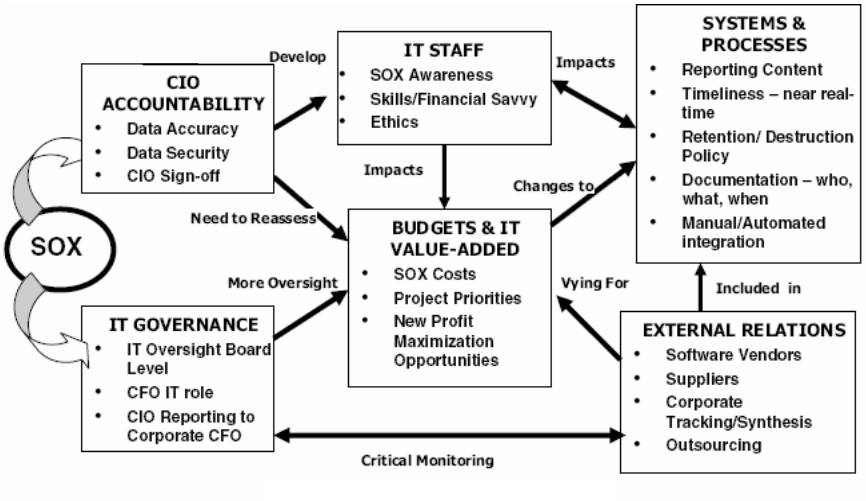

Figure 2.3: Impact of SOX (Source: Kaarst-Brown & Kelly, 2005, p.2).

[1]Separation of duties is a cornerstone in the protection of information assets and in preventing loss. The completion of a significant task that involves sensitive information should require two people. The check and balance method requires two or more people to conspire to commit an incident, which is known as collusion.

Feltham & Mbagwu (2006) argue that the legislation was necessary, relevant and effective. They observed that prior to the implementation of SOX over ten percent of five hundred companies examined were disclosing earnings in a potentially deceptive way. However in 2003 less than one percent of disclosed earnings were potentially misleading. SOX has, as a result, augmented investor confidence, corporate accountability and improved financial statements' transparency (Nazareth, 2006). IS expenditures are no longer justified due to their technical value but in clear business terms (View, 2003) adding to the value of the IS Security function.

SOX reforms require a broad, digital paper trail to authenticate corporate financial reports (View, 2003). Adherence to industrial IT best practices and standards can potentially minimise the controls and systems devoted to SOX compliance, reduce costs and free resources for the development and advancement of the business (Hackett, 2006). Companies have adopted best practice models or practices (Katz, 2006), such as capabilities maturity models (CMM), industrial standards such as COBIT (Control Objectives for Information and Related Technology), ITIL[2] and ISO17799 to assess internal practices (Poole, 2001; Mishra & Dhillon, 2008).The most effective approaches appear to be those that have been developed as an extension of the overall control structure of the specific organisation (Rittenberg & Senn, 1993). However Backhouse et al., (2006) contends that a clear mapping of IS Security requirements to policies can be found in ISO17799. As explained by Belsis et al., (2005) the standard has greatly influenced the perception of IS Security.

Conversely, Baskerville & Siponen (2002) contend that the use of standards in the development of best practices is disadvantageous. General IS Security management standards and guidelines fail to take into account that organisations differ and, as a result, managerial IS Security requirements are different (Baskerville, 1993). Standards additionally do not acknowledge the social nature of problems (Dhillon & Backhouse, 2001). Generic standards omit business requirements as they are broadly written to necessitate ad hoc managerial decision-making. Standards are fundamental compatibility specifications that shape the configuration, use and management of information systems (Backhouse et al., 2006). Standards are instruments of power as they contain inscribed actions and processes that influence organisational activities and work tasks. Standards have been the subject of several studies in the IS field (Baskerville, 1993; Dhillon & Backhouse, 2001; Siponen, 2005; Backhouse et al., 2006) and are of enormous importance in providing structure and guidance for specifying IS Security policies, controls and processes. They are however generic and rarely aligned to the needs of the organisation (Baskerville et al., 2005). IS Security functions and managers do depend on this guidance in applying suitable IS Security measures to comply with regulatory requirements (Baskerville et al., 2005; Sundt, 2006; Backhouse et al., 2006).

The following section explores the nature and scope of the formal models used for the technical specification of IS Security. Formal models are used to build security into computer-based systems and hence have limited utility in specifying technical controls alone. Thus, it is imperative to present the models available in literature and highlight such negative aspects prior to discussing the challenges facing IS Security and using knowledge management approaches to incorporate behavioural aspects of IS Security.

[2]The Information Technology Infrastructure Library (ITIL) is a customisable framework of best practices that promote quality computing.

2.4.5 Information Systems Security Methods and Models

This section highlights the fact that "…serious research into the nature of the management of information systems security is scarce" (Baskerville, 1994, p. 385). However from the technical view point there are a number of solutions available. One of the key issues in managing IS Security is secure information systems. However, despite the recognised relevance of IS Security (Baskerville, 1992; Straub & Welke, 1998; Anderson, 1999; Dhillon & Backhouse, 2001) the IS Security research community has become bogged down in small-scale technical questions (Dhillon & Backhouse, 2001; Siponen et al., 2008). To alleviate this issue several methods for the development of secure information systems have been proposed, ranging from checklists (Von Solms, 1999; Eloff & Von Solms, 2000a; Dhillon & Backhouse, 2001) to risk management (Siponen, 2005). Studies suggest that the alternative methods for developing and managing secure IS are influenced by the IS software development methods of previous generations (Baskerville, 1993; Dhillon & Backhouse, 2001). Interestingly the oldest approach, namely checklist-standard-based securing of IS (Baskerville, 1993) is still used. However even though checklists are not a hot topic in the IS Security literature; IS Security management standards (Baskerville, 1993; Dhillon & Backhouse, 2001) have received increasing attention from IS Security researchers and practitioners (Baskerville et al., 2005; Siponen, 2005; Dhillon, 2006).

Following ideas and developments in the field of software engineering new IS Security management-oriented maturity standards have been put forward, including the System Security Engineering Capability Maturity model (SSE-CMM, 1998). Greenstein and Vasarhelyi (2001) contend that risk management is a methodology for evaluating the prospects of future events that can exert grave outcomes. It involves the deployment of effective mechanisms for addressing these repercussions. The authors assert that it is not possible to eradicate risk completely. Ettinger (1993) argues that if risk management is properly carried out and combined with education and awareness initiatives, it might be the most cost-effective IS Security-enhancing measure available. Stoneburner et al., (2002) contend that the process enables IT managers to leverage both the cost efficiency of operations and economic costs of protective mechanisms. Each of these approaches is used in the systematic secure development of systems processing data, information or knowledge.

Organisations utilise IS Security models to secure their assets (Baskerville, 2004; Siponen & Willison, 2007). The IS Security market is glutted with an array of traditional approaches so much so that practitioners find it difficult to understand the differences between them (Siponen, 2005; Dhillon & Torkzadeh, 2006). The first model is the Trusted Computer System Evaluation Criteria (TCSEC) model. This examines issues pertaining to trust and the confidentiality of the data stored and is largely concerned with securing classified data when purchasing systems from vendors but it underplays the importance of contextual issues (Dhillon & Hossein, 2001; Whitman & Mattord, 2005; Dhillon, 2006). The criteria used lists different levels of a trusted system, from level D with no security to level A1 with high security. This strategy was also used in the Bell La Padula model (Sundt, 2006). This model deals with controlling access to objects. These are akin to applying read/write permissions to word documents. However the Denning information flow model is used to apply security to information flows. As explained by Dhillon (2006) the model is based on the assumption that information constantly flows, is compared and is merged. The model examines a set of objects (files) that contain information and identifies active agents who are responsible for information flows, allocates each a security class (confidential) and the security of

the objects responsible for merging information is decided. The Chinese wall model was designed to provide controls that mitigate conflict of interest in commercial organisations, and is built upon an information flow model. A Chinese wall or firewall is an information barrier implemented within a firm to separate and isolate persons who make investment decisions from persons who are privy to undisclosed material information which may influence those decisions. This is a way of avoiding conflict of interest problems.

The Observe-Orient-Decide and Act (OODA) model is regarded as a basic measure of the responsiveness of any security unit or function (Baskerville, 2004). The OODA loop has become an important concept in both business and military strategy. Essentially decision-making occurs in a cycle of observe-orient-decide-act. An effective function will sense (observe) a change in its setting, analyse the meaning and importance of the change (orient), identify the best strategy to take advantage of the change (decide) and then implement the change (act). An entity (either an individual or an organisation) that can process this cycle quickly, observing and reacting to unfolding events more rapidly than an opponent, can thereby "get inside" the opponent's decision cycle and gain an advantage (Baskerville, 2004). One of the most widely referenced and often discussed security models is the ISO17799 as a model for IS Security. This is viewed as a standard which fails to incorporate the human factor into IS Security (Baskerville, 2005). This exclusion of the circumstance of IS Security limits an organisations ability to protect all of its components.

Finally the security infrastructure in place must support the size and scope of the enterprise. The IS Security methodology adopted must allow for the growth/expansion of the organisation. In order to secure growing and emerging organisations IS Security researchers and IS Security managers need to develop emergent IS Security approaches (Baskerville, 2004). Like its organisational counterpart, emergent IS Security endures continual change while seeking stability but never achieving it. Therefore IS Security managers and functions must adapt to and respond to an emergent IS Security landscape. IS Security activities, aimed at protecting information/knowledge assets must be both defensive and offensive. Researchers have argued that IS Security can be treated like a game (Wang, 2007) between the IS Security group and hackers (Baskerville, 2004; Borodicz, 2005; Behara et al., 2005). The approaches to managing IS Security seem to dwell on the organisation as a machine metaphor (Walsham, 1991) and fail to consider stakeholder interests (Dhillon, 2006) and function activities such as KM.

2.4.5.1 IS Security Strategic Decision-making

At a corporate level the IS Security strategy determines key decisions regarding investment, diversification, and integration of resources in line with other business objectives. At a business level, the IS Security strategy analyses the threats and weaknesses of the IT and security infrastructure. In the IS Security literature, many of these issues have been investigated under the umbrella of risk analysis (section 2.4.1). The business IS Security strategy defines the overall approach to gain advantage from the environment, the detailed deployment of the procedures, at the operational level, is an issue of concern for functional strategies such as the IS Security policy. Current IS Security research considers policies as a vital component for the protection of the organisation. However, Wrapp (1991, p.32) contends that "good managers don't make policy decisions". Therefore the emphasis is on avoiding the danger of managers being trapped in disputes arising out of stated policies rather than binding IS Security to the

organisational objectives. The main IS Security objective is to create an environment where there is no scope for abusing organisational systems and processes.

One of the fundamental problems regarding IS Security is for an organisation to choose the right kind of environment to function in. Strategic IS Security issues relate to where the firm chooses to operate and the scope of the organisation's relationship with other organisations. For example if an organisation chooses to work with a U.S. based firm, the organisation will have to ensure compliance with corporate governance as mandated by the Sarbanes-and-Oxley Act of 2002 (section 2.3.1). Moreover, any change to an existing business process will have implications for business partners. In addition to corporate governance and environmental issues, IS Security return on investment (ROI) has become important (section 2.3.3). Addressing this issue would have a range of implications in ensuring IS Security. Investment in IS Security has increased, but so have the number and range of security breaches (CSI, 2009; 2010). This could mean that security mechanisms are ineffective (Figure 2.2), investments are being made in the wrong places or that the benefit of an ISS investment is intangible (Dhillon, 2006). Regardless of the reasons for a lack of security investment payoff, it is important that key decisions about security objectives are identified. While many organisations have engaged in identifying security issues and as a result developed appropriate IS Security policies, there is a clear mismatch between what the policy mandates and what is done in practice. Researchers have termed this as a gap: in espoused theory (actions that people write) and theory-in-use (what people actually do). Therefore theories-in-use have degrees of effectiveness which are learned (Mattia & Dhillon, 2003). Espoused theory and theory-in-use, as illustrated in Figure 2.4, are a part of the double-loop learning concept which creates a mindset that consciously seeks out security problems in order to resolve them. This results in changing the underlying governing variables, policies and assumptions of either the individual practitioner, function or the organisation.

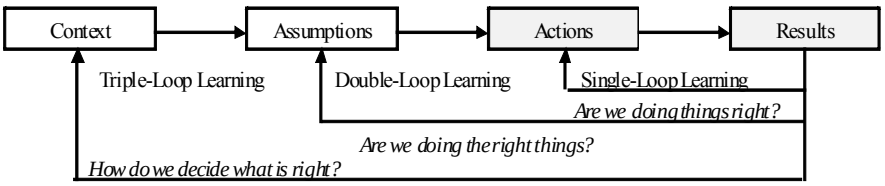

Figure 2.4: Levels of Learning

Fiol and Lyles (1985) categorise higher-level organisational learning as a double-loop process yielding organisational characteristics such as acceptance of non routine managerial and heuristic behaviour. In contrast, single-loop processes ignore any security contradictions as we tend to be blind to the counterproductive features of security actions. Therefore organisations exhibiting single-loop security; display minimal, if any, security contradictions in their underlying governing values, variables, policies and assumptions. Single-loop is categorised as lower level organisational learning yielding characteristics such as rules and routines. When using the double-loop learning security framework, assumptions underlying current espoused theories and theories-in-use are questioned and hypotheses about their behaviour are tested. The double-loop inquiry is very different from single-loop learning. The organisation and therefore the IS Security function must become aware of the security conflict regarding the actions that have produced unexpected outcomes. The IS Security function must

reflect on the conflict and become aware that they cannot correct the error using existing IS Security controls more efficiently under the existing conditions (Dhillon, 2006). It is vital to discover what conflict is causing an error and then to undertake the inquiry that resolves the security conflict. Therefore the restructured governing variables become inscribed in the espoused theories. This allows the espoused theories and theories-in-use to become similar and thus more susceptible to effective ISS realisation.

Thus, the following section presents the growing IS Security challenge of managing IS Security knowledge in the context of protecting an ever increasingly changing and complex organisations to strategically adapt their business environments.

2.5 The Information Systems Security (ISS) Challenge

The preceding sections focussed on a review of the IS Security literature examining its nature and importance, and the evolution of ISS to become a strategic function within organisations. The purpose of this section is to discuss IS Security from a knowledge management perspective (KM), describing the types, reservoirs and approaches used.

IS Security is threatened with ongoing managerial challenges internal and external to the organisation. The sheer complexity of modern organisations means that the management of IS Security failures and the implementation of IS Security controls (formal, informal and technical) are far from rare (Baskerville, 2004; Borodzicz, 2005; Randeree, 2006). IS Security functions (attempt to) ensure the protection of information resources or assets (Dhillon, 2006). As a result IS Security has become a priority for modern enterprises and organisations, as the majority of organisational processes and activities depend heavily on IS. The IS Security industry has responded by developing a plethora of tools and mechanisms covering almost every aspect of IS Security. However, the effectiveness of current IS Security solutions and best practice standards have been seriously questioned (Baskerville, 2005). IS Security challenges increase the importance of managing IS Security knowledge in the context of protecting the organisation. The goal in managing IS Security is to minimise information systems operational risks. This involves several activities, such as planning, designing, implementing, monitoring, reviewing, and improving (BSI, 2002). These activities require specialised IS Security knowledge and one of the challenges faced by modern organisations is to acquire and manage expert knowledge in the area of IS Security (Belsis et al., 2005).

Combining IS Security knowledge, activities, experts and tools could resolve the different IS Security challenges encountered by organisations (Sundt, 2006; Randeree, 2006; Huo et al., 2008). This could be achieved through the utilisation of an effective KM approach, a solution which has been ignored by academia and industry. The application of the strategy to the management of IS Security knowledge would enable a more holistic approach to the management of IS Security across the enterprise. The researcher proposes that the application of a KM approach to the management of IS Security knowledge could alleviate the challenges facing IS Security managers and functions. KMS have been proposed as possible solutions in capturing and storing IS Security knowledge (Jamieson & Handzic, 2004; Holsapple & Singh, 2004; Belsis et al., 2005; Randeree, 2006). However approaches incorporating people and processes as well as technologies have never been contextually investigated.

The administration and management of IS Security is a knowledge-intensive activity and to be effective must be managed. Research to date has focussed on incorporating IS

Security into IS development and ignores the social context of the phenomenon. The next section explores ISS from a KM perspective.

2.6 Information Systems Security from a KM Perspective

This section will define and differentiate between the different types of knowledge before discussing its various reservoirs and processes. The section will also discuss the mechanisms used to promote KM, the organisational infrastructure necessary to support it and the impact of managing knowledge for individuals, functions and finally the organisation.

Knowledge is distinct from data and information (Davenport & Prusak, 1998). Alavi and Leidner (2001), contend that some authors, mainly in IT literature, address defining knowledge by distinguishing between knowledge, information and data and also by setting out the perceived hierarchy or continuum of the three. Fundamentally data is "…a set of discrete, objective facts about events" (Davenport & Prusak, 1998, p.5). Knowledge is regarded as volumes of relevant information endowed with experience (Avison & Fitzgerald, 1997). An ISS expert, to be effective, must use extensively both formal (quantitative) and informal (qualitative) information (Earl & Hopwood, 1980; Land & Kennedy-McGregor, 1987) in decision-making. Finally, knowledge could be considered as "actionable information" (Jashapara, 2004, p. 16). Tiwana, (2000) contends that actionable information aids decision-making through the provision of information at the right place and time and in the format required by the decision-maker. However this view does not fully explain the characteristics of knowledge and theorists such as Wiig (1999, p. 32) oppose this view and posit that knowledge is fundamentally different from both data and information:

> "[Knowledge]…is consistent of truths and beliefs, perspectives and concepts, judgments and expectations, methodologies and know-how and is possessed by humans, agents or other active entities and is used to receive information and to recognize and identify; analyze, interpret and evaluate; synthesize and decide; plan, implement, monitor, and adapt – i.e. to act more or less intelligently. In other words, knowledge is used to determine what a specific situation means and how to handle it".

Therefore knowledge is used to convert data into information and information into knowledge. Some experts view knowledge as an object which can be easily managed and controlled (secured through access rights and partitioning) while others view it as a product of a complex interaction between human beings and information. There are, however, alternative views of knowledge. Knowledge can be viewed from an objective or subjective stance (Becerra-Fernandez et al., 2004). The objective view presents (IS Security) knowledge as an object with access to information or as a capability (Dhillon & Backhouse, 2001). The subjective view presents (IS Security) knowledge as a state of mind or as a practice. There is, however, a general consensus among theorists (Polanyi, 1966; Nonaka, 1994; Dieng et al., 1998; Coakes, 2004) that knowledge can be split into two different facets: (1) explicit and (2) tacit. Coakes (2004) posits that tacit knowledge is more difficult than explicit to codify as it is retained in people's minds and is not easily shared. The author advises that it is important to define the concept and different types of ISS knowledge before identifying its locations and discussing its application and management.

2.6.1 Types of IS Security Knowledge

Knowledge has been classified and characterised in a number of different ways. Alavi and Leidner (2001) categorise it as individual, social, casual, conditional, relational and pragmatic. In this section some of the more important classifications of (ISS) knowledge are discussed.

The first distinction is between tacit and explicit knowledge. Literature examining the application of tacit knowledge outlines how it can be identified and shared within organisations (Polanyi, 1966). Saint-Onge (1996) argues that the largest amount of knowledge within an organisation is tacit and is unarticulated. However, to be competitive an organisation must generate or create new knowledge. Knowledge is either tacit or rooted in tacit knowledge (Svieby & Simons 2002). Therefore, knowledge is not private but social (Polanyi, 1975). This "personal coefficient" shapes all factual knowledge and thereby bridges the gap between subjectivity and objectivity. Explicit knowledge is viewed as knowledge that is codified, documented, archived and communicated. Explicit knowledge can be easily transferred from one place to another in a systematic and structured format (Alavi & Leidner, 2001; Coakes, 2004). Bohn (1994) posits that explicit knowledge is more valuable than tacit knowledge and disseminated through more technologically enabled processes. The opposing view as advocated by Alavi and Leidner (2001) is that this is problematic, and derived from an inability to measure the true value of knowledge. Polanyi (1975) asserts that tacit knowledge forms the foundation that is necessary to understanding and structuring explicit knowledge. Therefore both present benefits and challenges to organisations (Alavi & Leidner, 2001; Holsapple & Singh, 2006). Stake (1978, p.6) provides one of the most succinct elaborations of this type of knowledge:

> Tacit knowledge is all that is remembered somehow, minus that which is remembered in the form of words, symbols, or other rhetorical forms. It is that which permits us to recognize faces, to comprehend metaphors, and to "know ourselves". Tacit knowledge includes a multitude of inexpressible associations which give rise to new meanings, new ideas, and new applications of the old.

The effects of globalisation and the accelerated rate of progress in technology have led to changes in the practices of the knowledge worker (Jashapara, 2004) or ISS practitioner. Changes such as advancements in ISS technologies have implications for the way IS Security practitioners work. When individuals work in groups or functions to perform tasks, those members create and apply tacit knowledge (Polanyi, 1966). Therefore explicit and tacit forms of knowledge are quite distinct. However, it is possible to convert explicit into tacit and vice versa.

The second classification of knowledge is between declarative and procedural knowledge. Declarative knowledge is factual information that is static and easily described. It is an explicit form of knowledge which actors are able to verbalise and is usually factual in nature. In direct contrast procedural knowledge is regarded as dynamic requiring skilled actions. This type of knowledge is not easily explained or verbalised. Essentially declarative knowledge is described as "knowing that" and procedural knowledge as "knowing what".

The third classification of knowledge focuses on whether the knowledge is possessed widely or narrowly (Becerra-Fernandez, et al., 2004). General knowledge is possessed by a large number of individuals and can be transferred easily. Specific knowledge (or

idiosyncratic knowledge) is possessed by a limited number of people and is both difficult and expensive to transfer (Hayek, 1945; Jensen & Meckling, 1996). Specific knowledge can be further broken down into technically and contextually specific knowledge. Technically specific is deep knowledge about a specific field through both training and applied experience, and contextual refers to the knowledge of particular circumstances, such as an ISS audit, of time and place in which tasks must be performed (Hayek, 1945). It cannot be acquired through training. The objective of most organisations, attempting to manage knowledge regardless of the type, is to capture, share, acquire, control and create explicit and tacit knowledge (Standards Australia, 2001).

However, the difficulty is in locating the different reservoirs of (declarative, procedural, general, specific, explicit and tacit) knowledge. Davenport and Prusak (1998) identified knowledge mapping as a crucial step in the codification of corporate classified knowledge. Sources of knowledge should be identified and evaluated to determine their use. Knowledge maps are therefore useful as an inventory of knowledge within the organisation. The maps are graphic directories of knowledge sources such as assets, structures, applications or development stages (Eppler, 2004). Knowledge can also be classified according to its role within organisations (Becerra-Fernandez, et al., 2004). Knowledge is divided into support knowledge, which relates to the organisational infrastructure and facilitates day-to-day operations; tactical knowledge, which relates to the short-term positioning relative to its business environment, competitors and suppliers; and finally strategic knowledge, which pertains to the long-term positions of the enterprise regarding its corporate vision and strategies in achieving that position. Table 2.6 outlines and categorises examples of sources of IS Security knowledge and their roles within an organisation as identified by Belsis et al., (2005).

Level of Abstraction	**Security Practice**	**Potential Sources of Related Knowledge**	**Target (Proactive/Reactive)**
Strategic	Design & dissemination of security policies	Policy document	Proactive security
Tactical	Risk analysis IS audit	Risk analysis documentation Documented countermeasures Audit trail reports, automatic logs Audit documentation & reports	Proactive security Reactive security Proactive security Reactive security
Operations	Security management tools NW security & Firewalls	Reports Alerts | Logs	Proactive security Reactive security

Table 2.6: IS Security Practices & Relative Sources of Security Knowledge (Source: Belsis et al., 2005, p.194).

2.6.1.1 Knowledge as Practice

Gherardi (2000, p.218) argues that "*practice connects knowing with doing*". Therefore knowledge practice is based on the assumption that activity includes inseparable physical and cognitive elements. As a result knowledge use and development is therefore regarded as a fundamental aspect of activity (Hislop, 2005), making knowledge inseparable from human activity (Orlikowski, 2002). Equally, all knowledge work, whether using knowledge, sharing knowledge, developing knowledge or creating knowledge will involve an element of activity. Blacker (1995, p.1023) explained it as "*something that people have, it is suggested that knowing is better regarded as something* [IS Security practitioners] *do*."

Schon argued that the skilful practice exhibited by professionals does not consist of applying some prior knowledge to a specific decision or action, but rather of a kind of knowing that was inherent in their action. The essential role of a human agency is knowledgeable performance. Maturana and Varela (1998, p. 27) similarly define knowing as: "effective action," and write that "all doing is knowing and all knowing is doing." When we focus primarily on knowledge, we lose the centrality of action in knowledge-ability. Schon (1983) suggests that the tendency to slip from a focus on knowing to that of knowledge is deeply rooted in our theoretical enterprise as we attempt to develop (and test) theories that make sense of (or predict) effective action.

Employee ongoing engagement in social practices, and thus their reproduction of the knowing generated in those practices, is how they reconstitute knowledge ability over time and across contexts. Continuity of competence, of skilful practice, is thus achieved not given (Orlikowski, 2002). Existing approaches to studying distributed organising tend to focus on the importance of knowledge transfer across boundaries, and the value of generating a set of "best practices" that can be propagated through the dispersed operations. A view of knowing as enacted in practice does not view competence as something to be "transferred," and suggests that the very notion of "best practices" is problematic. When practices are defined as the situated recurrent activities of human agents, they cannot simply be spread around as if they were fixed and static objects. Rather, competence generation may be seen to be a process of developing employee's capacity to enact what we may term "useful practices"-with usefulness seen to be a necessarily contextual and provisional aspect of situated organisational activity.

The next section discusses the different reservoirs of (ISS) knowledge (or stores) before discussing the approaches used to manage knowledge.

2.6.2 Reservoirs of IS Security Knowledge

Knowledge resides in several different locations or reservoirs of knowledge (Becerra-Fernandez, et al., 2004).They encompass people (individuals and groups), artefacts (practices, technologies and repositories) and organisational entities (organisations, functions, and inter-organisational networks).

Drucker (1993) contends that knowledge is always embodied in a practitioner, created, augmented or improved, applied, taught and shared by a person. A considerable amount of knowledge resides in **individual members** of the firm (Argote & Ingram, 2000). As a result the majority of organisations seek methods to retain knowledge which might be lost, through, for example staff turnover (Jamieson & Handzic, 2004). Knowledge work is the ability to create an understanding of the nature of organisations and processes and in the application of this understanding as a means of generating wealth (Boland & Tenkasi, 1995). Managers are needed to govern initiatives (Davenport & Prusak, 1998) in managing knowledge. These managers should be skilled in the management of projects, change and technology. Leadership (governance) is responsible for appointing and identifying individuals, such as a Chief Knowledge Officer (CKO), to identify knowledge assets and artefacts within the organisation (Davenport & Prusak, 1998; Jamieson & Handzic, 2004). However, IT auditors and IS Security Officers should also be involved in the process (Standards Australia, 2001) to assure that the processes are controlled.

A significant amount of organisational memory is stored in **organisational artefacts**. Some knowledge is stored in practices, organisational rules, routines and procedures

which are developed through experience over time, such as disaster recovery procedures (Levitt & March, 1988). Considerable knowledge is also stored in technologies and systems. In addition to storing data, IT and computer based information systems can store knowledge and facilitate relationships such as communities of practice (CoP). Knowledge stored in repositories represents another method of storing knowledge in artefacts. Knowledge repositories can be paper-based, embodied in books, white papers, and procedures or electronic such as web-based frequently asked questions (FAQ) and forums (Becerra-Fernandez et al., 2004).

IS Security knowledge is also stored within entities such as **organisational units**, the organisation itself and inter-organisational networks. The firm stores specific knowledge regarding: the norms, values, practices and culture which embody the organisation. To effectively understand the culture of an organisation (Section 2.3.4) it is necessary to examine the business environment; the organisation's mission, vision and values; technology; IS Security knowledge structures; management style and organisational structure; individuals; collectives or groups and organisational memory (Lemon & Sahota, 2004). The knowledge stored in units, such as a department represent the formal functions of individual stores of knowledge specific to a unit or function. Customer Support (CS) functions are regarded as knowledge-intensive units focussing on supporting the problem-solving needs of an organisation's customer base. The CS function of a multinational organisation is formed to capture and transfer the knowledge of their support experts, trouble-shooting and case-based reasoning (CBR) systems (Huang et al., 2007). Support functions predominately apply a form of a KM approach in supporting an organisations customer base (Becerra-Fernandez, et al., 2004).

ISSUE	SOURCES
Expertise Development	Seminars
	Scientific journals, international conferences and specialised websites
	International standards and guidelines from international organisations
Categories of ISS knowledge	
Organisational knowledge	On-the-job training
	ISO17799 categorisation
	Culture
	Organisation structure
	Organisational needs addressed by the IS perception of risk
	IS configuration and functionality

Table 2.7: IS Security Knowledge (Source: Belsis et al., 2005, p.195).

Knowledge transfer has extended from passing information from individual to individual (Cantoni et al., 2001) to moving knowledge around the organisation (Rutkowski, 1999). As a result the collective knowledge of a function is synergistic (Becerra-Fernandez et al., 2004). Knowledge is also stored in **inter-organisational relationships** such as collaborative partnerships. Table 2.7 outlines some of the sources of IS Security knowledge exploited in order to protect corporate boundaries. Additionally regardless of type or classification, knowledge provides substantial value to the organisation and it must learn to manage (Stewart, 1997) and to retain its value through control (Holsapple & Singh, 2004; Jamieson & Handzic, 2004; Randeree, 2006).

2.6.3 IS Security Knowledge Management Approaches

Knowledge Management (KM) is a holistic attempt to manage organisational assets through the effective utilisation of experts, technologies and processes in the business environment in which the company operates to achieve competitive advantage. Definitions of knowledge management abound. Table 2.8 provides an overview of some of the more well known definitions. However KM lacks an agreed upon definition (Ives et al., 1998) but is viewed as an important discipline which promotes the creation, sharing and leveraging of the organisations memory. This problem is mirrored in the IS Security literature (Section 2.2). IS Security lacks an agreed definition even though it is viewed as a vital discipline in protecting valuable corporate assets. For the purpose of this research, KM is concerned with ensuring that knowledge is available in the right form to the right processors (systems, people and processes) at the right time for the right cost (Holsapple & Singh, p.220).

KNOWLEDGE MANAGEMENT DEFINITIONS	VIEWPOINT	AUTHORS
"[Knowledge management]... draws from existing resources that your organisation may already have in place - good information systems management, organisational change management, and human resources management practices".	Integration of resources	Davenport & Prusk,1998
"…improving the ways in which firms facing highly turbulent environments can mobilise their knowledge base (or leverage their knowledge "assets") in order to ensure continuous innovation".	Strategy	Newell et al., 2002
[knowledge management] "is an array of process that deal with the creation, dissemination and utilisation of knowledge	Array of processes	Avital, 2004, p.2
"[knowledge management is]…the systematic organisation, planning, scheduling, monitoring and deployment of people, processes, technology and environment to facilitate the creation, retention, sharing identification, acquisition, utilisation and measurement of information and new idea, in order to achieve strategic aims"	Knowledge is a condition of access to information.	Lehaney et al., 2004, p.3
knowledge management is "in its broadest application refers to how a firm acquires stores and applies its own intellectual capital".	Intellectual capital	Wickramasinghe, 2003, p. 296
knowledge management is the most recent in a long line of fads and fashions embraced by the Information Systems community that have little to offer. Rather, we argue for a refocusing of our attention back on the management of data, since IT processes data – not information and certainly not knowledge.	A fad	Galliers & Newell, 2001, p. 609

Table 2.8: Definitions of Knowledge Management (KM).

Alavi and Leidner (2001) contend that the growing realisation of the value of organisational knowledge has driven organisations to transform themselves into knowledge-orientated enterprises (Wong & Aspinwall, 2005). Organisational knowledge is viewed as a strategic asset, because it meets the following criteria: it is valuable, rare, inimitable and non-substitutable (Holsapple & Singh, 2004). Prusak (2001) states the sceptics of KM argue that it was invented by consultants in response to declining revenues, a belief compounded by Galliers and Newell (2001) who view KM as the most recent in a long line of fads and argue for a refocus back to the management of data. This argument is mirrored in studies such as Butler (2000) as KM has resulted in as many successes as failures (Randeree, 2006). The benefits include leveraging core

business competencies, accelerating innovation and time to market, improving cycle times and decision-making, strengthening organisational commitment and building sustained competitive advantage (Davenport & Prusak, 1998). Avital (2004, p.2) posits that KM is composed of "an array of processes that deal with the creation, dissemination and utilisation of knowledge". There are many different ways in which KM can be practised and that certain KM approaches are more suited to particular organisations than to others. Holsapple and Joshi (2004) have identified various KM activities or processes. An examination of these activities revealed a great deal of variation, as a result many researchers use different terms for the same processes.

Therefore the following sub-sections describe the IS Security processes discussed in this study: IS Security knowledge acquisition, capture, creation, sharing, application/use and control.

2.6.3.1 IS Security Knowledge Acquisition and Capture

Alavi and Leidner (2001), and Davenport and Prusak (1998) agree that acquired or procured knowledge does not need to be created within the firm, just new to the firm. Knowledge acquisition is the process by which knowledge is obtained (Huber, 1991, p.90). Once it is identified it is transformed into a representation that can be internalised (Holsapple & Singh, 2004). The most effective acquisition method is simply to buy or lease knowledge. This has resulted in many companies encouraging employees to copy or develop ideas from other organisations through, for example, reverse engineering (Becerra-Fernandez et al., 2004). A takeover is an approach to acquiring knowledge (Davenport & Prusak, 1998). Knowledge can be acquired by "grafting" or employing new members with the skills and knowledge lacking instead of developing it in-house (Jashapara, 2004). Examples of knowledge acquisition include: conducting an external survey, training, purchasing data sets, monitoring the external IS Security landscape, network (NW) perimeter penetration testing, gathering knowledge via competitive intelligence (Holsapple & Singh, 2004) or information warfare (Baskerville, 2004).

Knowledge capture is "the process of retrieving either explicit or tacit knowledge that resides within people, artefacts, or organisational entities" (Becerra-Fernandez et al., 2004, p.33). The knowledge captured may reside inside or external to the organisation in the form of vendors, consultants, competitors, partners and past employees. It also utilises Nonaka's (1994) externalisation and internalisation to capture tacit and explicit knowledge.

2.6.3.2 IS Security Knowledge Creation

Davenport and Prusak (1998) regard knowledge creation as a sign of a healthy organisation becoming a learning organisation (Coakes, 2004), arguing that knowledge does not remain static. The knowledge that organisations collect must be maintained with a "focus on continually renewing existing knowledge, creating new knowledge, and effectively using that knowledge in … practices" (Oppong et al., 2005, p.431). A common method of generating knowledge is to establish dedicated resources for doing so, such as research and development (R&D) groups (Davenport & Prusak, 1998). Leveraging tacit knowledge is a difficult process and central to its attainment is the collaboration of the actors. To facilitate these processes the structure, management and the necessary ICT must support them. One of the primary factors for knowledge creation is a culture of learning. There are four modes of knowledge conversion

required for knowledge creation: (1) socialisation, (2) externalisation, (3) conversion and (4) internalisation (Nonaka et al., 1996).

1. **Socialisation** is the process by which tacit knowledge from one individual is converted into the tacit knowledge of another though observation and practice. Examples include: trial and error learning, on the job training, mentoring, direct or indirect communication.
2. **Externalisation** is the process of changing tacit knowledge into explicit through dialogue and group reflection.
3. **Combination** is a process of combining components of explicit knowledge to create and store in knowledge systems such as: KMS, databases and documentation, enabling additional members of the unit or organisation to access knowledge.
4. **Internalisation** is the process through which experts can personalise explicit knowledge and convert it into tacit knowledge.

Knowledge creation occurs when there is continuous interaction between tacit and explicit knowledge, producing a spiral effect, starting with one process and moving onto the new mode continuously. Knowledge creation examples include: making a decision, recognising or solving a problem, inventing a process, brainstorming, constructing a software routine and discovering a pattern.

2.6.3.3 IS Security Knowledge Sharing

Knowledge sharing is the process through which explicit or tacit knowledge is communicated between individuals, groups, units or organisations. In contrast, knowledge exchange or trading focuses on sharing explicit knowledge between groups and organisations (Grant, 1996). The goal of many organisations is to create communities where knowledge is shared and used by developing CoP (Pan & Leidner, 2003). Davenport and Prusak (1998) contend that when such networks share knowledge through a variety of communication tools such as: email, telephone or groupware, new knowledge is created. Davenport and Prusak (1998) recognise that knowledge is transferred within organisations whether or not the process is managed. Dieng et al., (1998) add that organisational memory must be distributed to the correct people either passively or actively. Davenport and Prusak (1998) posit that organisations should introduce knowledge sharing methods, adding that companies must expand on their idea of productivity in the workplace to include continuous learning, social interaction, and reflection by providing the time and recognition for employees.

2.6.3.3.1 Communities of Practice (CoP)

IS Security depends on professionals internal and external to the organisation such as '*Communities of Practices'*. These communities are composed of a group of individuals united by similar interest/values (Wenger, 2000). Communities of practice (CoP) develop as individuals interact frequently to discuss topics of mutual interest and demonstrate the productive value of knowledge in groups. Wenger and Snyder (2000, p. 139) define communities of practice as "*groups of people informally bound together by shared expertise and passion for a joint enterprise*". Additionally they explain that "*managers cannot mandate communities of practice. Instead, successful managers bring the right people together, provide an infrastructure in which communities can thrive, and measure the communities' value in non-traditional ways*". Communities appoint their own leaders but they require a significant amount of support both from senior management and in terms of infrastructure and funding.

One of the strengths of the communities of practice approach is that it can be applied in a wide range of organisational settings. However, this can also be viewed as a weakness, since it may encourage its inappropriate application (Roberts, 2006). In contrast, Kimble and Hildreth (2004, p. 5) question whether communities of practice are always suitable for the business setting, arguing that their interests may not be aligned with those of the organisation and 'because they are self-managed and self directed, their contribution to the organisation will always be uncertain'. Workers increasingly operate in an individualistic world of weak ties where resources are frequently obtained through personal networks rather than through organisation based communities. Individuals belong to a variety of communities of practice some internal to their work organisation while others will be external arising from their personal and professional networks. Therefore for businesses and organisations to fully leverage their knowledge capacities they must harness communities of practice within and external to their organisations. Given that knowledge is transferred through social interaction, then businesses need to pay particular attention to their recruitment and training policies to ensure that they maintain an appropriately skilled workforce to maximise the advantages of these communities. Another limitation to the approach is; its relevance for small and medium sized organisations. Communities of practice require cultivation if business organisations are to fully exploit their positive attributes (Wenger et al., 2002); they will not flourish in inhospitable organisational environments.

As explained by Pan and Leidner (2003) the goal of KM initiatives in many organisations is to develop networks where knowledge is shared and used by developing these communities of practice (CoP). Davenport and Prusak (1998) argue that when networks such as these share enough knowledge over time, new knowledge is generated within the organisation and that these networks are usually brought together through a knowledge champion or by a variety of communications tools such as groupware. Buchel and Raub (2002) identified the importance of building trust within these communities of practice in order for tacit knowledge to be passed from one member of the network to another. Buchel and Raub (2002) add that in this context, trust can be considered the foundation on which knowledge is generated within these networks. It is through the manipulation of an organisation's culture and politics, that employees can be easily influenced as the most important influence on staff attitude is a demonstration of the commitment to IS Security by key opinion formers in each functions (Gaunt, 2000). Therefore it is the role of managers to support the goals and objectives of the organisation not the (information/knowledge) society which forms the organisational context (Borodzicz, 2005). However, due to the political nature of knowledge, this can be problematic.

2.6.3.3.2 The Political Nature of Knowledge

Malhorta (2003, p.3) contends that "…*knowledge has no definitive value but can potentially be of use indefinitely*." Therefore even though knowledge is difficult to quantify it is a significant component of the decision making process as "…*it does have a clear impact on business outcomes*" (Soo et al., 2002, p.129). Intangible assets, such as knowledge, are difficult to appraise but researchers argue that they should not be ignored (Conway, 2004; Ulrich & Smallwood, 2004). Brelade and Harman (2003) contend that the drivers for KM are much the same as drivers for change in any organisation; to obtain a competitive advantage. As the majority of organisations regard the knowledge possessed by the firm as an asset. It is therefore the management,

creation and application of this knowledge that is a direct contributor in achieving and maintaining a sustainable competitive advantage (Stewart, 1997). Additionally Coakes (2004) argues that knowledge workers, aided through the implementation of a knowledge management initiative, can make more effective decisions and improve their efficiency and therefore in turn improve the profitability of the organisation through the effective management of knowledge. Brelade and Harman (2003, p. 31) states that "*an emphasis on knowledge, skills and creativity and on the capturing and sharing of information, are all issues that impact upon how people are managed*". However knowledge is power and some individuals see more benefit from hoarding their knowledge than sharing it, unless knowledge sharing is rewarded more than knowledge hoarding (Davenport & Prusak 1998; Walsham 2001). The decision knowledge workers face regarding whether or not to participate in knowledge related activities has been compared to a classical public good dilemma.

In summary knowledge workers would have access to a shared organisational resource (a public good) whether they contributed to it or not and its value would not diminish from its use. The dilemma for knowledge workers is that there are potentially positive and negative consequences to both sharing and hoarding knowledge. The advantages of sharing knowledge is intrinsically rewarding at both group (increased performance) and organisational levels. The monetary rewards (bonus) and an individual's status can be enhanced. Consequently, the negative implications vary from loss of power and time. Moreover, knowledge sharing is dependent on the motivational elements of the knowledge sharing process and the culture in which the process operates. Raghu and Vinze (2005) added that knowledge sharing can be successful even without a set structure for knowledge sharing, as long as there is a context for the knowledge initiative. However the benefit of hoarding knowledge is that the practitioner avoids the risk of giving away knowledge, power and status that are aligned to the knowledge.

A general weakness of KM initiatives is that the issues of conflict, power and politics are generally neglected (Hislop, 2005). The potential for conflict between workers and management can shape individuals willingness to participate in organisational knowledge processes. Therefore inter-personal and inter-group conflict in organisations can also affect KM processes. Hislop (2003) identified a number of instances where organisational change was hindered by a lack of willingness to share across functions. This can often be explained due to a history of inter-functional conflict and competition. Furthermore Hislop et al., (2000) found that knowledge and personal networks are used by many practitioners as political tools in support of particular objectives. This is compounded by the work of Buchanan and Gibb (2008) where political behaviour has been found to be a common feature of organisational life. However the importance of conflict, power and politics in impacting workers willingness to share is profound. They are a common feature of organisational life and due to the inter-relationship between power and knowledge, knowledge is a resource workers make use of in dealing with situations of conflict.

2.6.3.4 IS Security Knowledge Application and Use

The process of knowledge application relies on available knowledge. The better the other processes of knowledge (acquisition, capture, creation, sharing and control) the better the application of knowledge. Knowledge application involves the use of knowledge to guide decisions and actions. The use of knowledge benefits from two processes: routines and directions (Grant, 1996). Routines involve the use of knowledge embedded in procedures, rules and norms that guide the user. Direction refers to the

approach through which the individual possessing knowledge directs the action of another employee without transferring the knowledge. If knowledge is used or applied the possibility exists that organisational learning is innovative and as a result adds value to the organisation (Holsapple & Joshi, 2004).

2.6.3.5 IS Security Knowledge Control

Knowledge control processes ensure that needed knowledge resources and activities are available in sufficient quantity and quality. These are also subject to, as identified by senior management, the required protection and constraints (Holsapple & Singh, 2004). The goal of knowledge control is the "[protection from] ...loss, obsolescence, unauthorised exposure, unauthorised modification, and erroneous assimilation [which] is crucial for the effective management of knowledge" (Holsapple & Joshi, 2000, p.240). To protect information or knowledge assets, management must allocate appropriate IS Security and control measures to counter known threats (Jamieson & Handzic, 2004; Becerra-Fernandez et al., 2004; CSI, 2009). The risks to KM are numerous. Intellectual property (IP) is regarded as the results of a human intellectual (KM) process which has inherent value to the organisation that sponsored the process (Becerra-Fernandez et al., 2004). Organisations create and support the development of IP as part of a knowledge creating process and have control of the tangible representation of those ideas. The more codifiable, documented and distributed the knowledge the greater the risk or compromise. Therefore intellectual property losses for an organisation can occur in a variety of ways (Becerra-Fernandez et al., 2004; CSI/FBI, 2006), such as: employee turnover, physical theft of sensitive propriety documents, inadvertent disclosure to third parties and reverse engineering..

Companies can use nondisclosure agreements (NDA), patents and copyrights to reduce KM risks (Jamieson & Handzic, 2004). Deliberate "acts of espionage" represent a broad category of electronic and human activities that breach the confidentiality of information (Jamieson, 1991; Whitman, 2003; Jamieson & Handzic, 2004). An unauthorised individual gaining access to corporate knowledge reservoirs is categorised as a deliberate act of espionage or trespass. The modification, deletion or insertion of KM information when passing through a network poses serious risks to KM (Jamieson & Handzic, 2004). Jamieson (1991) identified additional KM exposures such as an inability of KM software and hardware to recover or start, a lack of knowledge-use histories (audit trails) in hard or soft copy, inadequate trace facilities in KM software for debugging and testing, KMS knowledge not based on the best expert's knowledge, reasoning and explanations, inadequate control of and access to KM repositories, poor management of KM applications and inadequate training and supervision of KM personnel. IS Security controls are vital in assuring the quality and quantity of knowledge resources. Control is a managerial influence on KM to assure knowledge validity (accuracy and consistency) and knowledge utility (relevance and importance), (Jamieson & Handzic, 2004; Holsapple & Singh, 2004). Knowledge control should be a priority as the value of knowledge and the returns achieved depends on its effectiveness (IT Governance Institute, 2001; Randeree, 2006). Controls are therefore used as IS Security countermeasures to perceived threats to the operations of an organisation, be it the management of knowledge, information or data (Section 2.4.3).

The next section discusses the mechanisms used to promote KM before discussing the organisational infrastructure (Section 2.6.5) necessary to support, for example, the management of IS Security knowledge.

2.6.4 KM Mechanisms for IS Security

KM mechanisms are structural methods used to promote the use of KM tools. Mechanisms can be technological and non-technological. They are supported by the KM infrastructure and facilitate KM systems (Becerra-Fernandez et al., 2004). KM mechanisms range from on-the-job training, learning by training, face-to-face meetings, mentoring, employee shadowing, employee rotation, brainstorming and analogies. The processes discussed in Section 2.6.3 are facilitated by a number of KM mechanisms. Mechanisms which facilitate socialisation includes: cooperative projects across departments, repositories of best practices, lessons-learned and apprenticeships. Combination is facilitated through the collaboration of documentation, databases, problem-solving and web-based access to data. Knowledge capture is facilitated by case-based reasoning (CBR) tools and expert systems. Knowledge sharing utilises repositories, lessons-learned systems and expertise locators. Knowledge application systems such as expert and decision support systems and hierarchical relationships in organisations, Help desks and support centres are used to facilitate direction, and policies and standards are used to support routines.

Davenport and Prusak (1998) argue that KM is about much more than just technology, but concede that technology is an important enabler. At the heart of the systems dimension of KM is the shift from a technology focus to people and their contribution when knowledge is made accessible through technology. Tyndale (2002) states that; the goal of KM tools or systems is to facilitate the process. Additionally Croasdell (2001) contends that there are advantages in using IT to support corporate memory, as the contents stored are explicit and can be shared and modified if required. However Tyndale (2002) argues that organisations are not reaping the full benefits of KM-enabling tools. Many of the KM systems utilised in firms seem to provide elaborate document management more than effective KM. As explained by Davenport and Prusak (1998) the term "KM technologies" encompasses a number of technologies including web-based systems, Lotus notes and artificial intelligence (AI) systems, such as expert systems, case-based reasoning (CBR) and neural networks. The typical goal of a KM initiative is to capture knowledge in a documented form and store it into a repository where it can be easily stored and retrieved by knowledge seekers. Davenport and Prusak (1998) identified three basic types of knowledge repositories: external knowledge (competitive intelligence), structured internal knowledge (for example: research reports, product-orientated marketing materials and methods) and informal internal knowledge (discussion databases full of "lessons-learned"). Davenport and Prusak (1998) did not identify expert systems in their research even though these can also be classed as repositories of narrow knowledge domains.

The combination or integration, along with the capability to combine an expert's experience in the form of a system is regarded as a strategic tool (Alavi & Leidner, 2001). Systems capable of combining explicit and tacit knowledge of workers are referred to as KM Systems (Butler & Murphy, 2007). These systems are used to acquire and manage knowledge and distribute it among functional units as well as with any external collaborating functions. KMSs are used to disseminate and reuse knowledge creating new knowledge through the use of the system (Alavi & Leidner, 2001) improving the effectiveness of decisions (Peterson, 1996).

The next section describes the organisational infrastructure necessary to support KM.

2.6.5 Organisational Infrastructure

Organisational infrastructure is the foundation on which KM resides. It is composed of organisational: structure (Section 2.3.1), culture (Section 2.3.4), IT infrastructures, common knowledge and the physical environment (Standards Australia, 2001; Jamieson & Handzic, 2004). Common or general knowledge refers to cumulative experiences which support communication and coordination through common language, vocabulary, recognition of individual knowledge domains and shared norms (Grant, 1996). The physical environment is important as it allows employees to meet and share ideas and knowledge. A supporting organisational culture helps motivate employees to understand the benefits of KM. Knowledge sharing and use varies from one culture to the next (Davenport & Prusak, 1998). Traditional reporting relationships can influence the flow of data, information, knowledge and the nature of functions in making decisions and in sharing knowledge (DeSanctis, 1987; Dhillon, 2006). A CoP is a self-organised group of individuals dispersed geographically or organisationally but who communicate for problem-solving. Specialised structures and functions such as the IS Security and Customer Support functions specifically support organisational operations. IT and IS Security infrastructures also facilitate KM. IT infrastructures include data processing, storage, systems and ICT. It is the IS Security infrastructure which secures the organisation and assures the role, value and utility of its knowledge. It secures and supports the processes, people and technology involved to prevent uncontrolled organisational knowledge (Holsapple & Singh, 2004; Jamieson & Handzic, 2004; Belsis et al., 2005; Randeree, 2006). Knowledge assurance refers to a review of KMS and IT infrastructure to determine if the systems are secured. KM governance committees and IS Security functions are responsible for auditing KM (Jamieson & Handzic, 2004) for assurance.

2.6.6 KM Impact

Brelade and Harman (2003) contend that the drivers for KM are much the same as drivers for any organisational change striving for competitive advantage. Therefore IS Security knowledge "…has no definitive value but can potentially be of use indefinitely" (Malhorta, 2003, p.3). Even though knowledge is difficult to quantify it is a significant component of the decision-making process as "…it does have a clear impact on business outcomes" (Soo et al., 2002, p.129). Alavi and Leider (2001) highlight the fact that the greatest approach to sustainable competitive advantage is not the amount of corporate knowledge stored but the firm's ability to retain and ultimately disseminate the corporate knowledge-base and enhance existing knowledge resources. KM can impact organisations and organisational performance on the following levels: individuals, functions, processes, products and the overall performance of the organisation (Becerra-Fernandez et al., 2004).

Employee performance can be greatly impacted through KM. It can facilitate employee learning and enhance their exposure to the latest knowledge in their fields of expertise through for example access to experts and lessons-learned from a project. Employees are also encouraged to learn from one another to adapt to changes in their environment. These improvements also enhance job satisfaction as skills are improved, as is the employee's market value (Brown & Duguid, 1991). Additionally KM facilitates improvement in organisational processes such as manufacturing and engineering by improving the effectiveness, efficiency and innovativeness of the different processes. Specifically KM enables organisations and their functions to adapt quickly to changes

in their environments, such as the IS Security landscape and technological advancements.

Choi and Lee (2002) argue that the relationship between KM processes and strategies is critical to improving corporate performance. KM impacts the organisation's products by adding value or creating knowledge-based products and services. Essentially existing products are improved to add value to the organisation, and knowledge-intensive services such as support functions (Nonaka & Takeuchi, 1995). By overlooking the need to formulate a clear business case, many KM implementations have resulted in failure (Coakes, 2004). KM can impact the organisation either directly, through for example, increased revenue or indirectly in exploiting intangible assets which are difficult to measure (Smith & McKeen, 2004). Hansen et al., (1999) warn against companies isolating KM in functional departments such as Human Resources, IS Security or CS. The co-ordination of KM requires the leadership of senior management if the organisation and its customers are to benefit from its utilisation. Even though many researchers highlight the importance of an overall KM strategy (Hansen et al., 1999; Choi & Lee, 2002; Malhotra, 2000; Coakes, 2004) few are implemented. The majority of organisations focus on the operational side of KM as opposed to an integrated approach. However if knowledge positively impacts an organisation and is therefore valuable then it should be secured (Holsapple & Singh, 2004; Jamieson & Handzic, 2004; Belsis et al., 2005; Randeree, 2006; Guo, 2008). To do so IS Security functions need to be effective and proactive in responding to IS Security issues. Therefore managing IS Security knowledge is vital in meeting IS Security challenges (Belsis et al., 2005; Guo, 2008).

The next section discusses the importance of managing IS Security knowledge and the research lens identified from the literature discussed in this Chapter.

2.7 Managing Information Systems Security Knowledge

Trends such as continued IT evolution and new business models coupled with strategies, such as KM, have resulted in complex business environments (Baskerville & Siponen, 2002; Patterson, 2005). Researchers, investigating knowledge and its management, have to include the protection and security of knowledge (Randeree, 2006). IT governance is advocated by Ramos (2001) as a key enabler in aligning the environment to the objectives of the organisation. Jamieson & Handzic (2004) posit that IT and IS Security governance should involve the governance of KM to ensure that it is aligned to the strategy of the organisation. The IS Security function should be consulted when considering IS Security controls for KM technologies, people and processes. These personnel are responsible for identifying vulnerabilities and abuses associated with KM systems (Whitman & Mattord, 2005) and the implementation of appropriate controls to alleviate identified threats. Considerable risk is posed in establishing a KM initiative within the organisation (Section 2.4.1). KM processes, technologies and knowledge workers should also be framed to identify the risks, if any, in generating, capturing, acquiring, sharing and applying knowledge.

To effectively secure tangible and intangible assets such as knowledge, IS Security knowledge must be successfully managed to ensure that IS Security practitioners and senior management are equipped to meet any IS Security risk and challenge. However the IS Security literature focuses on technical subfields with the majority on automatic mechanisms on such as IS Security technologies, access controls (Castano et al., 1995; Booz et al., 2005; Borodzicz, 2005; Balta & Gaadingue, 2006; Siponen & Willison,

2007), cryptography (Kahn, 1996; Menezes et al., 1999; Dhillon, 2006), and development methodologies for secure information systems (SIS) (Baskerville, 1988; 1993; 2005; Dhillon, 1997; Dhillon & Backhouse, 2001). A detailed analysis of all of the different themes of IS Security is lacking (Siponen, 2005). Andress (2004) contends that IS Security involves people (Adams et al., 1992; Siponen, 2000; Hinde, 2003; Belsis & Kokolakis, 2005), processes and technologies. Von Solms (2001) warns that if IS Security is not addressed in a holistic and comprehensive way significant risks to the organisation will continue to emerge. Understanding IS Security is still at a theory-building stage (Dhillon & Backhouse, 2001; Siponen et al., 2008), especially when incorporating KM (Belsis et al., 2005; Randeree, 2006; Guo, 2008). In order to gain an understanding of where further research is required, it is necessary to examine and synthesis previous research findings which was the purpose of this Chapter. The next section discusses the research lens identified from the synthesised IS Security and KM literatures.

2.7.1 Research Lens

The objective of this research is to determine how IS Security could leverage the concept of KM. The research lens (Figure 2.5), derived from the IS Security and KM literatures discussed, is used for conceptualising and operationalising the factors of this study. Figure 2.5 illustrates the variables identified and used as a guide to explore the objective of this research. Each variable is tagged with its corresponding subsection to illustrate the flow of the research lens. The research focuses on the relationship between IS Security and KM and the proposed benefits that an IS Security KM initiative would produce. In conceptualising the research lens, the researcher followed DeLone and McLean's (1992; 2003) advice in identifying an outcome to determine the propositions to be explored and the (inter-dependent) relationships which exist between them. The DeLone and McLean IS success model is based on a review and integration of a hundred and eighty research studies that used some form of system success as a dependent variable. The outcome of this investigation is ultimately to apply a KM approach to IS Security. An analysis of contrasting (IS Security and CS functions) approaches to the management of knowledge - through the operationalisation of the model will explain how the methods applied in one context can be transferred to the context of other functions with predicable tangible benefits.

KM assessment approaches usually combine several measures. One such approach involves the application of benchmarking or comparing knowledge management at an organisational or subunit level with other organisations or subunits. Benchmarking can be adopted as a systematic technique for evaluating a company's or function's performance towards its strategic goals. Benchmarking is based on the recognition that best practices are often the same within the same company and within the same industry. Benchmarking within the same company, the same industry or competing firms. High performing units and companies can be studied and their practices replicated within another unit or company. Therefore, in benchmarking KM at the Customer Support (CS) subunit level with another of the organisations subunits IS Security in order to replicate the success of KM in other unit. Additionally, an analysis of the approaches used by these specialised structures in managing knowledge within and across the two case studies will facilitate benchmarking at organisational level to determine how ISS can leverage the concept of KM within and across the case organisations.

The systematic evaluation of the CS and ISS functions approaches, used to manage knowledge, will enable an assessment and replication of the approaches used to ultimately improve how IS Security knowledge is managed. The replication of the case study protocol (CSP) illustrated in Figure 3.2 and discussed in Chapter 3 presents a cross-case analysis of the different approaches to managing knowledge, these can then be synthesised to determine any comparisons, differences and impacts across the two organisations investigated. Additionally through the exploration of the interplay between the functions (ISS and CS) at a local level and across the two case studies, a possible correlation between KM and IS Security could be identified, presenting a possible competing outcome to this study.

The remaining sub-sections outline the different components of the research lens (Figure 2.5). The first three describe the types (Section 2.7.1.1), reservoirs (Section 2.7.1.2) and approaches (Section 2.7.1.3) used to manage knowledge, each of which is inter-dependent on the other. Section 2.7.1.4 describes the KM mechanisms needed to promote KM in organisations. Section 2.7.1.5 describes the levelled (individual, functional and organisational) impact of the approaches used. Finally, section 2.7.1.6 describes the infrastructure needed to support the management of knowledge in a competitive business environment.

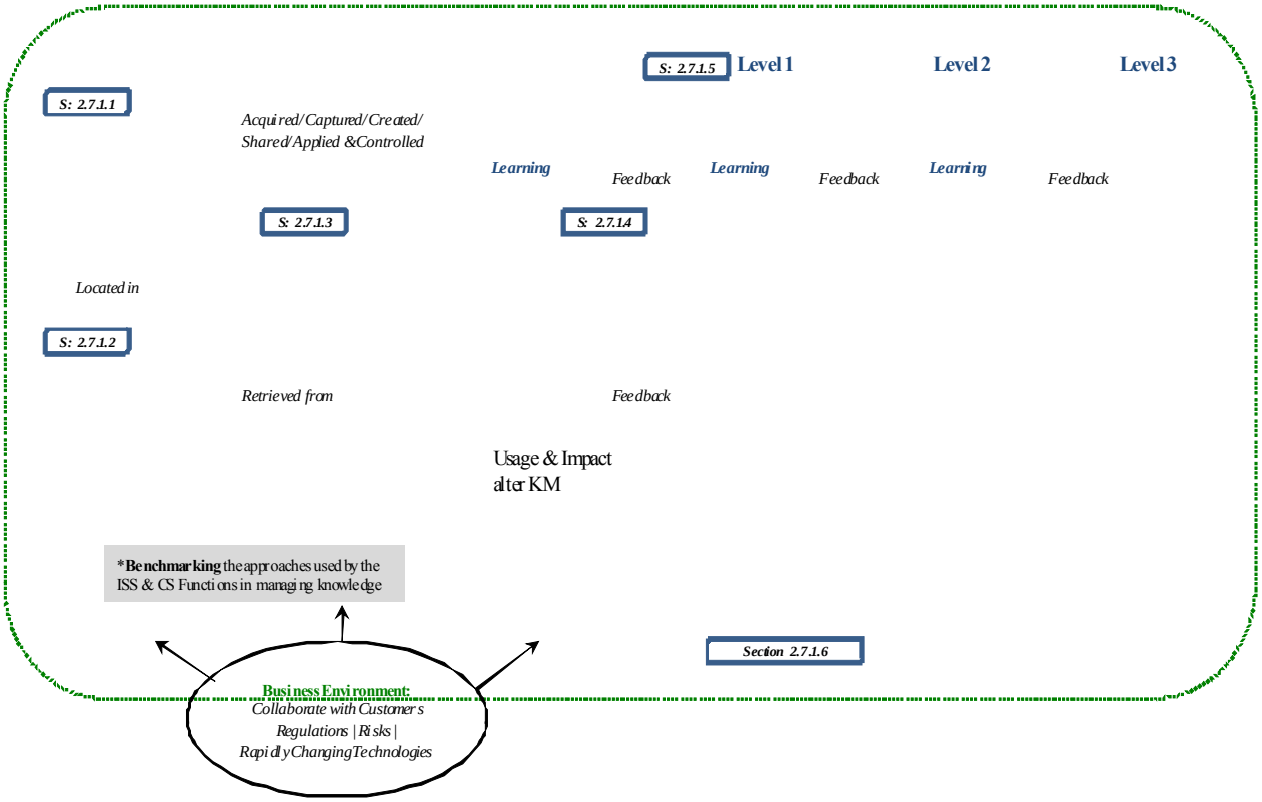

Figure 2.5: Conceptual Model – KM Approach to IS Security

2.7.1.1 Types of IS Security Knowledge

Knowledge has been classified and characterised in a number of different ways. Figure 2.5 illustrates the types of ISS knowledge as an inter-dependent variable in the conceptual model created. Literature examining the application of tacit knowledge outlines how it can be identified and shared within organisations (Polanyi, 1966). Explicit knowledge can be easily transferred in a systematic and structured format (Alavi & Leidner, 2001; Coakes, 2004). The practices of the ISS practitioner have changed due to technological advancements (Jashapara, 2004) and when individuals

work in functions to perform tasks, those practitioners create and apply tacit knowledge (Polanyi, 1966). Tacit and explicit can therefore be further classified as declarative and procedural. ISS Knowledge can be either possessed widely (general) or narrowly (specific) (Becerra-Fernandez, et al., 2004). Specific knowledge (technically or contextually) is possessed by a limited number of people and is both difficult and expensive to transfer (Hayek, 1945; Jensen & Meckling, 1996). Knowledge can also be classified according to its role within organisations (Becerra-Fernandez, et al., 2004). As a result knowledge is divided into operational (facilitating the day-to-day operations); tactical knowledge (which relates to short-term positioning relative to its business environment); and finally strategic knowledge (which pertains to the long-term position of the enterprise). The next section describes the different reservoirs of ISS knowledge as illustrated in Figure 2.5.

2.7.1.2 Reservoirs of IS Security Knowledge

IS Security knowledge resides in people, artefacts and organisational entities (organisations, units, inter-organisational networks). A considerable amount of knowledge resides in individual practitioner (Argote & Ingram, 2000) and extensive knowledge resides within functions. Regardless of type or classification, knowledge provides substantial value to the organisation and it must learn to manage (Stewart, 1997) and to retain its value through control (Holsapple & Singh, 2004; Jamieson & Handzic, 2004; Randeree, 2006). Knowledge is pulled from its various stores and processed through: acquisition, creation, sharing, application, use and control. Therefore knowledge is always changing and should never be static. As a result the better the approach used to manage knowledge the better its creation and use.

2.7.1.3 IS Security KM Approaches

The objective of most organisations is to acquire, capture, create, share, apply and control explicit and tacit knowledge (Standards Australia, 2001). Alavi and Leidner (2001), and Davenport and Prusak (1998) agree that acquired knowledge does not need to be created within the firm, just new to the firm. Knowledge capture is "the process of retrieving either explicit or tacit knowledge that resides within people, artefacts, or organisational entities" (Becerra-Fernandez et al., 2004, p.33). Davenport and Prusak (1998) regard knowledge creation as a sign of a healthy organisation becoming a learning organisation (Coakes, 2004). Knowledge creation occurs when there is continuous interaction between tacit and explicit knowledge, producing a spiral effect, starting with one process and moving onto the new mode continuously. Knowledge sharing is the process through which explicit or tacit knowledge is communicated between individuals, groups, units or organisations. The goal of many organisations is to create communities where knowledge is shared and used by developing CoP (Pan & Leidner, 2003). The process of knowledge application relies on available knowledge. If knowledge is used or applied the possibility exists that organisational learning is innovative and as a result adds value to the organisation (Holsapple & Joshi, 2004). Knowledge control processes ensure that needed knowledge resources and activities are available in sufficient quantity and quality. These are also subject to, as identified by senior management, the required protection and constraints (Holsapple & Singh, 2004). To protect information or knowledge assets, management must allocate appropriate IS Security and control measures to counter known threats (Jamieson & Handzic, 2004; Becerra-Fernandez et al., 2004; CSI, 2009). The risks to KM are numerous. Controls are therefore used as ISS countermeasures to perceived threats to the operations of an

organisation, be it the management of knowledge, information or data. The next section discusses the mechanisms used to promote KM as illustrated in Figure 2.5.

2.7.1.4 IS Security KM Mechanisms

Use of KM mechanisms, in the context of this research, is measured in terms of the change which occurred as a result of managing knowledge either unintentionally or purposefully (O'Dell et al., 2004). The use of KM in either a general or specific context will affect its success. A causal relationship between KM and use exists (Gartner, 2000). If the level of use increases then the approach used will have a greater impact on the users (individuals and functions) and therefore the organisation (DeLone & McLean, 1992). The combination or integration, along with the capability to combine an expert's experience in the form of a system is regarded as a strategic tool (Alavi & Leidner, 2001). The next section describes the levelled impact of KM as illustrated in Figure 2.5.

2.7.1.5 IS Security KM Impact

KM can impact organisations and organisational performance on the following levels: (1) individual, (2) function processes, products and ultimately the overall performance of the organisation (Becerra-Fernandez et al., 2004). Employee performance can be greatly impacted through KM. It can facilitate employee learning and enhance their exposure to the latest knowledge in their fields of expertise. KM enables organisations and their functions to adapt quickly to changes in their environments, such as the IS Security landscape and technological advancements. KM can impact the organisation either directly, through for example, increased revenue or indirectly in exploiting intangible assets which are difficult to measure (Smith & McKeen, 2004).

2.7.1.6 IS Security Organisational Infrastructure

Organisational infrastructure is the foundation on which KM resides. As a result it is composed of organisational: structure (Section 2.3.1), culture (Section 2.3.4), IT infrastructures, common knowledge and the physical environment. However if knowledge positively impacts an organisation and is therefore valuable then it should be secured. To do so IS Security functions need to be effective and proactive in responding to ISS issues. Therefore managing IS Security knowledge is vital in meeting ISS challenges.

This research lens is a representation of the ISS and KM literature discussed in this chapter. Figure 2.5 illustrates the flow between the different variables identified. The different types of ISS knowledge are retrieved from the corporate knowledge reservoirs and manipulated /altered by the processes outlined. The application and use of knowledge enables the creation, sharing and reuse of every type of knowledge stored in the different reservoirs. These are then promoted through non-technological and technological mechanisms which in turn impact individuals, their groups and ultimately the organisation itself. Additionally, as this step-by-step cycle continues learning occurs is enhanced and alters the cycle of managing knowledge facilitated or hindered by the organisation infrastructure within a competitive business environment.

2.8 Conclusion

Chapter 2 identifies and describes the calls from academia and industry for an integrated approach to managing IS Security in order to provide the present study with a firm theoretical foundation. IS Security is a challenging research area in the context of IS yet it is under-researched. As the business and IS Security landscape changes, management must have the ability to make decisions based on judgement, understanding and knowledge. Traditionally there have been technocratic approaches to IS Security. Due to the continued increase in incidents and challenges to IS Security, the solution to better IS Security may not be found through technical measures. There is a pressing need for a theoretical framework against which practitioners may diagnose problems, plan action, adapt to a changing IS Security landscape and implement solutions. Existing IS Security models and procedures do not exhibit a high degree of flexibility, and as a result managers and IS Security practitioners make IS Security decisions in a knowledge vacuum. Risk can be managed or reduced when IS Security managers, practitioners and functions are aware of the full range of controls (formal/informal/technical), environmental threats, regulations, standards, technologies and practices available and implement the most effective solution. Threats should be met when organisations avoid reactive solutions and instead adopt proactive practices. To tackle threats or risks IS Security functions need to keep their skills and knowledge current. Therefore this thesis endeavors to explore the possibility of applying a KM approach to the management of IS Security knowledge. Table 2.9 outlines the family of definitions required for this investigation.

	DEFINITIONS
Organisations	can be viewed as being composed of the informal, formal and technical interconnecting parts or systems.
IS Security	is a process that ensures the protection of information resources encompassing the people, processes and technologies used.
KM	is concerned with ensuring that the knowledge is available in the right form to the right processors [systems, people and processes] whenever required
Culture	is enhanced coordination and control, improved goal alignment and increased employee effort
Explicit K	is codified, documented, archived and communicated
Tacit K	cognitive (beliefs, viewpoints and mental maps) and technical (know how)
Procedural K	is dynamic requiring skilled actions – knowing what
Declarative K	is factual information that is static and easily described – "knowing that"
Tech Spec K	deep knowledge about a specific field through training and applied experience
General K	possessed by a large number and can be transferred easily
Operational K	day-to-day operations
Tactical K	the short-term positioning relative to its business environment
Strategic K	to the long-term positions of the enterprise regarding its corporate vision
Reservoirs of K	encompass people, artefacts and organisational entities (organisations, functions, and inter-organisational networks
K Processes	is based on the assumption that activity includes inseparable elements
Acquisition	process by which new knowledge is obtained
Capture	process of retrieving knowledge that resides within people, artefacts /org entities
Creation	Generating knowledge
Sharing	explicit or tacit knowledge is transferred
Application	the use of knowledge to guide decisions and actions
Control	protection of knowledge resources
Mechanisms	are structural methods used to promote the use of KM tools
Impact	change striving for competitive advantage

Table 2.9: Root Definitions

CHAPTER THREE

THE RESEARCH STRATEGY

3.0 Introduction

Chapter three is about the theory, research question and model underlying this research (Figure 1.1). It sets out the research lens (Figure 2.5) informed by a review of the literature and defines the research objective and the research questions (Section 3.1). The philosophical perspectives of epistemology and the different methodologies are discussed in Section 3.2. After reviewing the different perspectives and considering the current state of research in the IS Security field, an interpretivist approach using qualitative methods was considered the most appropriate for exploring the management of IS Security knowledge. Section 3.3 describes the research strategy utilised. Section 3.4outlines the method by which the data was analysed from within and across the cases selected. The Chapter concludes with a summary of the research protocol, steps and time line (Section 3.5).

3.1 Framing the Research

The purpose of this section is to outline the research framework which is informed by evidence sourced from the literature and acts as a lens for this research study. Section 3.1.1 describes the framework used. Section 3.1.2 states the research objective. Section 3.1.3 concludes the section by formalising three research questions and explaining the purpose of each research question in the context of this study.

3.1.1 The Research Framework

Figure 2.5 illustrates the variables identified from the IS Security and KM literatures and was used as a guide to explore the objective of this research. Section 2.7.1 described the propositions, their measurements and the inter-dependent relationships which exist between them. In the context of this study, the literature provides a lens whereby operational factors and outcomes can be differentiated based on their applications within the two case studies. The factors and outcomes identified in the literature act as a basis for grounding the investigation of the approaches used to manage knowledge in two specialised IS Security and CS functions within the two organisations participating in this study. This equipped the researcher with a fitting lens, based on prior research, from which to initiate the investigation while allowing enough scope to enable additional factors, outcomes and implications to emerge from the contextual settings of the organisational environments participating in this study.

3.1.2 Research Objective

IS research seeks to describe, explore or explain a phenomenon expected to add value to the existing body of theory (Marshall & Rossman, 1989). Fundamental to this process is the identification of the research topic or objective (Jenkins, 1985; Mumford, 1985; Fitzgerald, 1991; Adam & Healy, 2000; Ghauri & Gronhaug, 2002; Saunders et al.,

2003) that will add to existing or create a new body of knowledge. The objective must be a clear and unambiguous statement to enable the researcher to select an appropriate research strategy (Jenkins, 1985). The accuracy of the research objective enables focused decisions to be made at critical stages of the research process. The primary objective of this study is:

> To explore how Information Systems Security (ISS) could leverage the concept of Knowledge Management (KM) through qualitative research.

3.1.3 Research Questions

Defining the research questions is one of the most important steps to be taken in any research (Benbasat et al., 1987; Miles & Huberman, 1994). A clear research question expresses the nature of an inquiry, allowing the researcher to link easily a study to its practical and theoretical contributions, and thus forming the backbone of relevant research design (Goldkuhl, 1996). However the research questions must also be questions that can be answered in a useful way (Drake et al., 1998). Therefore it is important to ensure that research questions are appropriate in terms of their interest, significance and value to the practitioner, the IS Security, and information systems research communities. The literature review facilitates the definition of the research questions as well as the research objective. To accomplish the research objective the following three research questions were formulated:

RQ.1: How can the organisational infrastructure support the management of IS Security (ISS) knowledge?

A review of the literature reveals the importance of the organisational infrastructure in providing the foundation on which the functional units within reside and operate. The review reveals five main components (culture, structure, common knowledge, IT infrastructure and physical environment) that are traditionally depicted as interconnecting parts of an organisational infrastructure. The researcher also identified the importance of the infrastructure in supporting the management of knowledge. However, research has yet to explore their application in supporting the management of IS Security knowledge. The purpose of this research question is to use this theory as a lens to examine how the organisational infrastructure supports the management of ISS knowledge in each organisation participating in this study.

RQ.2: How do the two functional areas IS Security (ISS) and Customer Support (CS) manage knowledge?

The literature suggests that the management of knowledge can directly impact the organisation at several levels: (ISS) individuals, the functions within, and the overall organisational performance. Impacts can come about directly from KM approaches or from the knowledge created, shared and applied through the approach. Therefore it is important to investigate how an organisation manages knowledge to determine the contribution of KM efforts. It is impossible to properly investigate this at an organisational level given size, uncertain business environments, and structural complexity. However examining how one function using a KM approach, producing quality knowledge solutions, within an organisation can help establish a baseline for implementing the KM approach, including the infrastructure and the mechanisms that can help support the management of knowledge, in another function. As Customer Support (CS) functions have been identified as knowledge intensive environments in the

literature they were selected as units or functions of analysis for this study. A similar review of literature revealed that research has yet to explore how IS Security functions manage IS Security knowledge. Therefore in comparing the KM approach used in a CS function with the IS Security function operating within the same organisation allowed the researcher to additionally determine how IS Security functions manage knowledge. The purpose of the second research question is to determine how KM can be used to manage IS Security knowledge within and across the two organisations participating in this study.

RQ.3: How can firms align Information Systems Security (ISS) to a Knowledge Management (KM) environment?

This question will be answered from within and across the two cases. A review of the literature revealed that there is little if any accord regarding the relationship between IS Security and the management of knowledge other than the application of ISS controls in the technological application of KM and vice versa. It is however agreed that both KM and IS Security involve people and processes as opposed to just technology. Therefore an organisation, through its ISS function, must align ISS to every facet of a KM environment to ensure that needed knowledge resources and processors are available in sufficient quantity and quality subject to the corporate ISS measures and constraints. An organisation that intends to stay in business must have the necessary IS Security controls in place to prevent and certainly to decrease the frequency of loss. The purpose of the third research question is to determine how firms align IS Security to a KM environment.

The three research questions described required the researcher to investigate the phenomena within their real contexts. Thus, an in-depth study of the context in which Customer Support and ISS functions manage knowledge is required (Section 3.5).

3.2 Research Philosophy and Methodology

Research philosophy and methodology guide the research strategy and prior to undertaking a research study a researcher must be familiar with the various assumptions that exist relating to ontology, epistemology and methodology as they define a researcher's belief about reality. This section establishes the philosophical perspectives of ontology (Section 3.2.1) and the epistemological positions of the interpretivist and positivist paradigms (Section 3.2.2). The methodological debate of quantitative versus qualitative approaches is then discussed (Section 3.2.3). Finally, this section justifies the research approach selected in the context of the current IS Security literature and concludes that due to the exploratory nature of this research, an interpretivist approach combined with qualitative data is the most suitable approach for exploring how IS Security could leverage the concept of KM.

3.2.1 Ontology

Ontology is the study of the essence of a phenomena "...and the nature of their existence" (Gill & Johnson, 1997). It is important for researchers to establish their ontological position as it will influence their research approach (Easterby-Smith et al., 1991). The ontology debate is divided between nominalism and realism. The nominalist perspective centres on the assumption that "...the social world external to individual cognition is made up of nothing more than names, concepts and labels which are used to structure reality" (Burrell & Morgan, 1979). The realist position assumes that the

"...social world external to individual cognition is a real world made up of hard, tangible and relatively immutable structures" (Burrell & Morgan, 1979). There is a range of possible ontological assumptions that underpin social enquiry and as a result the majority of researchers do not take an extreme position. Thus, the majority of research studies are conducted from a perspective somewhere between the two positions.

3.2.2 Epistemology

Epistemology is the basis for this search for reality and it refers to the assumptions about knowledge and how it can be obtained (Hirscheim, 1992). Gill and Johnson (1997) define it as "…the branch of philosophy concerned with the study of the criteria by which we determine what does and does not constitute warranted or valid knowledge". There are two major research philosophies which have dominated the discussion on research methodologies in the IS field including: positivist (sometimes called scientific) and interpretivist (also known as anti-positivist) (Galliers, 1992). When deciding between the two approaches, researchers must question their own beliefs about what knowledge is and how to validly acquire it (Hirschheim, 1985). The two research paradigms are discussed in detail in the following sections as failure to consider IS philosophical issues will negatively impact the quality of an investigation (Easterby-Smith et al., 1991).

3.2.2.1 Positivist Paradigm

Positivism is traditionally the dominant information systems research approach used (Orlikowski & Baroudi, 1991). Burrell & Morgan (1979) posit that positivism seeks to explain and predict what happens in the social world by searching for regularities and casual relationships between its elements. It is founded on the belief that the study of social systems should be carried out in the same way as the natural sciences (Walsham, 1993) and has evolved from a scientific tradition, where scientific approaches assume that observations of the phenomena under investigation can be made in an objective and rigorous manner (Galliers, 1991). Positivists believe that reality is stable and can be observed and described from an objective viewpoint (Levin, 1988). Human innovation and reasoning are excluded and research is carried out independently of the researcher (Klein & Lyytinen, 1985) and is therefore unaffected by irrationality, emotionalism and human fallibility (Checkland, 1981). The positivist paradigm asserts that there is a reality to be studied, captured and understood and this is an apprehensible reality which is assumed to exist, driven by unchallengeable natural laws and mechanisms (Guba & Lincoln, 1994). Positivist theory is generally quantitative in nature when testing theories to try and increase the predictive understanding of phenomena. It studies empirical/quantitative data by testing theories and hypotheses and quantifying variables and propositions (Orlikowski & Baroudi, 1991). It is characterised by reductionism, repeatability and refutation, and emphasises rigour and objectivity of method (Checkland, 1981; Hirschheim, 1985). This approach may not be suited to all research and its applicability and validity has come into question (Klein & Lyytinen, 1985). Despite the enthusiasm for scientific methods, there has not been a lot of success when they have been applied to social sciences (Hirschheim, 1992) such as the IS field where the relevant knowledge required cannot be acquired by applying traditional scientific methods so this approach is of little relevance to a qualitative study.

Due to the rich context of this study, the difference in research subjects and the fundamental differences in the study of people and other research are important factors (Nissen, 1985; Hirschheim, 1985; Klein & Lyytinen, 1985). The positivist approach

results in objectivity and testability by stripping the subject of context from meaning in the process of developing quantified measures of phenomena resulting in a lack of a deeper understanding of the phenomena (Guba & Lincoln, 1994). If the objective is to explore a phenomenon and investigate how IS Security could leverage the concept of KM through a comparative analysis of IS Security and CS functions then a method that will allow the collection and analysis of rich in-depth data is required. Thus, interpretive research has emerged as an important perspective from which to conduct information systems security research.

3.2.2.2 The Interpretivist Paradigm

The interpretivist approach to research is qualitative rather than quantitative; the approach analyses every aspect of human behaviour rather than on the collection of raw data. An increasing number of researchers have expanded their research beyond mathematical analysis to the studying of the environment of the problem at hand (Galliers, 1992). Research conclusions, using the interpretivist method, can be subjective and the researcher may be biased in the interpretation of participant's information, distorting the information so as to point it in a certain direction (Orlikowski & Baroudi, 1991). Another criticism is that it abandons testability of results so as to gain greater meaning from the research (Lee, 1989). The participants involved in a study may be misleading or deceptive when relaying their experiences and accounts of events and if a study is relying on these findings, it will be inaccurate (Orlikowski & Baroudi, 1991). Bharadwaj (1996) argues that the interpretivist approach is suitable for IS research because: (1) it reflects the link between the "human element and the technological aspect of IS research", (2) it contests the positivist view that IS development is purely technical, and (3) it encourages the use of a number of research methodologies for IS research. Remenyi et al., (1998) contend that researchers must be mindful of the weaknesses of their preferred approach to adequately build on the existing body of knowledge.

Table 3.1 outlines the fundamental differences between the two main IS paradigms regarding the patterned set of assumptions concerning reality (ontology), knowledge of that reality (epistemology), and the approach to knowing about the reality (methodology) in question. Walsham (1993) further differentiates between the two paradigms by stating that the interpretative approach describes a need to understand the phenomenon while positivism is purely technical. Positivism is also characterised by the scientific principles of repeatability, reductionism and refutability (Checkland, 1981). The scientific nature of positivism serves to test theory through controlled methods in order to prove both replicability and predictability with the researcher in the role of an observer as if a laboratory experiment was under scrutiny.

Klein & Lyytinen (1985, p. 137) highlight this meticulous approach when they state that:

> "To achieve both it teaches respect for facts, i.e. to refrain from armchair speculation when relevant facts can be brought to bear on issues. In using facts to support inferences, it puts the emphasis on rigor that is on intersubjectivity, reliability and reproducibility. These criteria are closely related and are to ensure that all trained observers at all times should be able to reach the same conclusions".

The authors do criticise the paradigm for applying scientific methods (as in the physical sciences) to a social science which eliminates the context of the research as well as rich descriptions eliminating the relevance of the research to invested parties. Galliers (1991) identified the following reasons for the inapplicability of the positivist approach for IS research concerning a social phenomena as: (1) the possibility of a number of different interpretations of the phenomenon; (2) the impact of the researcher on the social system under investigation and (3) the problems linked to forecasting future events where human behaviour is concerned.

QUESTION	POSITIVISM	INTERPRETIVIST
Ontological	Naive realism, "real" but apprehendable.	Relativism, local and specific constructed realities.
Epistemological	Dualist / objectivist; findings true.	Transactional / subjectivist; created findings.
Methodological	Experimental / manipulative verification of hypotheses, chiefly quantitative methods.	Hermeneutical / dialectical, mainly qualitative with support from quantitative methods.

Table 3.1: Basic beliefs of the two main paradigms (Source: Adapted from Guba & Lincoln, 1994)

Researchers are obliged to produce "… an understanding of the context of information systems and the process whereby the information system influences and is influenced by its context" (Walsham, 1993, p. 4). Galliers & Land (1987) posit that the interpretative approach can eliminate most if not all of the limitations associated with positivism to aid researchers in exploring the social nature of IS research. It too has critics, with the limitation of bias and incorrect interpretations (Kaplan & Duchon, 1988) among the most noted. Both paradigms (and every research method) possess limitations but it is the incorporation of appropriate research methods that can ensure not only the rich descriptions provided through the interpretative approach but the rigor and relevance of a more scientific approach (Drake et al., 1998).

In aiding the researcher it is Galliers (1991) who proposes a useful framework that compares and contrasts the positivist and interpretivist approaches and enables the researcher to assess the suitability of each in the context of the research topic being studied. The framework conceptualises the different stages of theory development and sees the progression of the IS field as being dependent on the development and advancement of theories relating to the underlying phenomena. Galliers (1991) also divides IS theory development into three stages: (1) theory building, (2) theory testing, and (3) theory extension. Theory building sees the use of qualitative techniques as the most appropriate to explore the different phenomena occurring. As more knowledge about the field is acquired and theory development becomes more advanced, quantitative techniques are used to test relevant hypotheses and to extend the existing hypotheses. As theory development moves from theory building to theory extension the type of research approach required shifts from exploratory and descriptive to confirmatory and predictive. Galliers (1991) argues that both the positivistic and the interpretivistic paradigms are applicable to IS research but are dependent on the stage of theory development in the area that is being studied.

The study of human behaviour and the complexities of the environment are also necessary in this research and cannot be understood with the use of quantitative methods alone. Lee (1997) argues that human and organisational instantiations of IT do

not have counterparts in the physical subject matters of the natural sciences and are therefore elusive in quantitative studies. As IS Security and KM are relatively new areas in IS, as such they should not be constrained by the limitations of quantitative analysis as opposed to the value added interpretive or qualitative approach which will enabled the researcher to explore both in the context of an organisational setting.

3.2.3 Methodological Debate: Quantitative Vs. Qualitative Studies

Qualitative techniques can provide the researcher with contextual information. Researchers advocate the use of case-based exploratory research (Guba & Lincoln, 1994) in providing rich descriptions of the phenomena under study. Through the use of interviews and document analysis the researcher is equipped to understand the problem situation and possess greater insight into the actor's perspectives (Guba & Lincoln, 1994). Van Maanen et al., (1982) conclude that qualitative methods guarantee the researcher greater quality in the research findings as the methods put more emphasis on the areas under study. The research method employed by the researcher depends largely on the research objective (Jenkins, 1985). Marshall and Rossman (1989) regard qualitative research as the most appropriate approach for exploring a phenomenon and for providing rich holistic descriptions. Despite the risk of data overload and researcher bias qualitative data is the source of grounded, rich data which has meaning to researchers and practitioners alike rather than pages of summarised numbers (Miles & Huberman, 1994). Denzin and Lincoln (1998, p. 3) define qualitative research as a "…multi method in focus, involving an interpretative, naturalistic approach to its subject matter". Due to the context of this study, the human and organisational aspects of the process must be analysed through the use of qualitative exploratory research. Thus, Section 3.2.4 further justifies the chosen research methodology by examining it in the context of current research in the IS Security field.

3.2.4 Justifying the Research Approach

The selection of the most appropriate research strategy is vital to the success of any study (Jenkins, 1985). This study is centred on how IS Security could leverage the concept of KM, therefore the researcher sought to use qualitative research to study the targeted functions in their natural settings where it can be interpreted to give meaning to the social context of the research (Gable, 1994; Lee, 1991). Quantitative approaches focus on a narrow set of variables ignoring important information regarding the social context of the research (Checkland, 1981; Guba & Lincoln, 1994). The exploratory nature of this study seeks to understand the potential use of KM approaches to manage IS Security knowledge. Social factors must be taken into consideration in IS research. Galegher et al., (1990) highlight the need to pay attention to the underlying fact that IS is not solely a technical discipline (Galegher & Kraut, 1990; Galliers, 1993), and that the end-users must be involved in the process. The purpose of a research strategy is the attainment of the research objective and the selection of an appropriate research strategy is of critical importance to the quality and value of the research (Jenkins, 1985). If sufficient exploratory studies have been carried out to identify meaningful relationships among variables to suggest testing hypotheses, the purpose of the research is testing, and, if insufficient exploratory research has been carried out for meaningful hypothesis generation, then the purpose of research is discovery.

3.3 Research Strategy: Case Study

There is no universally applicable methodology to answer any research question and enable the results to be beneficial to the field (Galliers, 1991). There are numerous methodologies for researchers to choose from (Jenkins, 1985). Consideration must be given to finding the research methodology to match the research objective (Jenkins, 1985; Davis, 1992). This section explains the research strategy adopted for this investigation which is, as previously stated, qualitative by nature. Section 3.3.1 discusses in detail the most appropriate methods for such a study. Case studies are discussed. The weaknesses of the approach are outlined and a two case organisations and a pilot case study approach is argued as a solution which possesses all of the benefits while eliminating the limitations of the single case approach (such as bias). This case approach facilitates replication and extension of the phenomenon among the two case studies while additionally allowing for cross-case analysis. The selection of the different sites is discussed in Section 3.3.2, to emphasise the importance of both IS Security and KM as are the diversities of each site. The section concludes by discussing the limitations of the chosen research strategy and how the researcher alleviated these through the application of rigorous data analysis (Section 3.3.3).

An explanation of the chosen strategy begins by providing an overview of the different research methods as depicted, particularly by Marshall and Rossman (1989), before discussing in detail the methods deemed appropriate for exploratory research. Oliasen (1991, p. 253) contends that:

> "The purpose of exploratory investigation is to move toward a clearer understanding of how one's problem is to be posed, to learn what are appropriate data, to develop ideas of what are significant lines of relation, and to evolve one's conceptual tools in the light of what one is learning about the area of life concerned with, for instance information systems".

Marshall and Rossman (1989), provide a framework to help researchers find the most appropriate match to the research objective. The framework, outlined in Table 3.2, is an effective aid to evaluate the different research approaches. The framework illustrates that the purpose of the research can range from the exploratory to the predictive. The investigation of how IS Security could leverage the concept of KM is a new phenomenon. The framework provided by Marshall and Rossman (1989), indicates that the research is exploratory. Benbasat et al., (1987) argue that IS researchers should study systems in practice because a substantial amount of IS research lags behind the knowledge practitioners have in the field which is certainly the case in the IS Security community. The case study approach stresses the importance of understanding empirical data in natural settings (Eisenhardt, 1989). The approach is a suitable choice in the study of IS issues and practice in general. The research strategy or plan adopted to operationalise the research is often a mesh of methods to alleviate the weaknesses identified in literature such as bias and the reliability of research findings. Easterby-Smith et al., (1991) argue that knowledge of the different research traditions enables researchers to adapt the chosen design to cater for constraints such as limited access to the data or a lack of prior knowledge of the topic.

Purpose of the Research	Research Question	Research Strategy	Examples of Data Collection Techniques
Exploratory To investigate little understood phenomena. To identify / discover important variables. To generate hypotheses for further research	What is happening in this social program? What are the salient themes, patterns and categories in participants" meaning structures? How are these patterns linked with one another?	Case Study Field Study	Participant Observation In-depth Interviewing Elite Interviewing
Explanatory To explain the forces causing the phenomena in question To identify plausible causal networks shaping the phenomena.	What events, beliefs, attitudes and policies are shaping this phenomenon? How do these forces interact to result in the phenomena?	Multi-site Case Study History Field Study Ethnography	Participant Observation In-depth Interviewing Survey Questionnaire Document Analysis
Descriptive To document the phenomena in question	What are the salient behaviours, events, beliefs, attitudes, structures and processes occurring in these phenomena?	Case Study Field Study Ethnography	Participant Observation In-depth Interviewing Document Analysis Unobtrusive Measures Survey Questionnaire
Predictive To predict the outcomes of the phenomena To forecast the events and behaviours resulting from the phenomena	What will occur as a result of these phenomena? Who will be affected? In what way?	Experiment Quasi Experiment	Survey Questionnaire (Large samples) Kinesics/Proxemics Content Analysis

Table 3.2: Matching Research Questions with Strategy (Source: Marshall & Rossman, 1989, p. 78).

3.3.1 Single Case Vs. Two Case Design

Robson (2002, p. 178) defines a case study as:

> "…a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence".

A case study is an in-depth examination of a single organisation, function or individual (Davis, 1992) which examines the relationships between variables in their natural setting (Benbasat et al., 1987) with no control exercised over the variables involved and which utilises a number of different methods of data collection (Benbasat et al., 1987). The number of case studies used is dependent on the research objective and contextual IS Security research is rare and required (Siponen et al., 2008). A number of authors argue that it is important to re-examine the nature and scope of the IS Security problem (Dhillon & Backhouse, 2001; Baskerville, 2005; Gerber & Von Solms, 2005). They suggest that the issue with current approaches for managing and investigating IS Security relates to the technical orientation of the solutions which focus on security mechanisms such as passwords and firewalls without examining the social elements involved in IS Security. The approach is an appropriate research method when the theoretical base of a particular research area is in its early stages (Benbasat et al., 1987), and is also appropriate in answering "how" and "why" questions (Yin, 1984; Benbasat et al., 1987). One of the primary benefits of the case study approach is that it facilitates the study of IS in a natural setting (Benbasat et al., 1987; Gable, 1994) thereby enabling theories to be generated from practice. The approach allows the researcher to gain an insight and understanding of the nature and complexity of social phenomena while maintaining a holistic and meaningful focus (Stake, 1994).

The case study approach is believed to be one of the "weaker" social science methods as it can lose rigour in its quest to gain relevance and context (Yin, 1989) but to increase the rigour of the case study approach a number of "logical tests" can be applied by which its research design quality can be judged (Benbasat et al., 1987; Lee, 1989; Yin, 1989; Walsham, 1993). These tests are "construct validity", "internal validity", "reliability", and "external validity or generalization". "Construct validity", which involves establishing correct operational measures for the concepts, ideas, and relationships being studied (Yin, 1989) and mapping clearly defined theoretical concepts and relations into empirical operations (McGrath, 1984), can be achieved through the use of multiple sources of evidence, the use of a chain of evidence, or by utilising a key informant to review a draft case study report (Yin, 1989). "Internal validity", which involves the explanation of causal relationships where certain conditions are shown to lead to other conditions, can be tested using such methods as pattern-matching, explanation building, and time series analysis (Yin, 1989). "Reliability" involves demonstrating that the procedures involved in carrying out a study (for example data collection procedures) can be repeated with the same results.

Errors and biases should be minimised by conducting research as if you are being observed (Yin, 1989). "External validity" refers to the applicability of the results of the study to another environment and population (Jenkins, 1985; Yin, 1989), while Lee (1989) explains "generalization" as a quality which describes a theory that has been tested and confirmed in another setting. Case studies rely on analytical generalisation (as opposed to statistical generalisation) where the researcher is endeavouring to generalise a particular set of results to some broader theory (Yin, 1989). In addition, a simply constructed case study can enable the researcher to challenge an existing theory and provide a source for new hypotheses (Saunders et al., 2003) which is one of the objectives of this research.

The case study method is a rich and valuable source of data, and is well suited to explaining the relationships between variables in their given context as required by descriptive research (Leedy, 1997). A single case study was considered, but the weakness of this is that it is restricted to a single organisation (Galliers, 1991). The use of more than one case study is more suitable when the research objective is more descriptive and is concerned with theory building (Yin, 1984). Two case studies allow for increased insight into the variables being researched. Benbesat et al., (1987) argue that more than one case is more appropriate than a single case when the objective of the study is to build and generate theory. The ability to cross-compare cases, obtain data from another source and integrate these "patterns" with literature provides the researcher with the opportunity to generate theory or knowledge with a reduced level of researcher bias. Although most, if not all, of the research gathered on IS Security has been quantitative by nature (Siponen, et al., 2008), KM studies have been for the most part qualitative but few, if any, have examined how IS Security could leverage the concept of KM. A two case design, incorporating a pilot case study, could aid in ensuring the research findings to strengthen the research (Benbesat et al., 1987). Literature does not provide any guidelines but rather recommendations regarding the number of cases (Patton, 1990).

Even though the research argument has a fairly strong theoretical basis, the choice of the cases is expected to advance the knowledge of the phenomenon and the theory. This assertion is especially true of case studies where the case itself provides a supportive role and facilitates understanding. As explained by Stake (1994) "the case is often looked at in depth, its contexts scrutinised, its ordinary activities detailed...because this

helps us pursue the external interest". As discussed by Walsham (1993), Yin (1994) and Lillis and Mundy (2005), the choice of a research method is based on the ontological and epistemological stance adopted. Hence, the strategy adopted in this research is purely qualitative and case based. Walsham (1993, p.15) argues in favour of case research as follows:

> "...from an interpretive position, the validity of an extrapolation from an individual case or cases depends not on the representativeness of such cases in a statistical sense, but on the plausibility and cogency of the logical reasoning used in describing the results from the cases, and in drawing conclusions from them".

Therefore a two case organisational design using a pilot case study to test the case study protocol (section 3.5) was chosen to investigate how IS Security could leverage the concept of KM. This strategy reduces the restrictions of a single case while incorporating the benefits. It complements the qualitative nature of this research, as does the selection of appropriate sites. Section 3.3.2 describes the selection of the case organisations.

3.3.2 Sampling of the Cases

Miles and Huberman (1994) contend that qualitative research typically involves purposive selection and not random sampling. The selection of a suitable research case study is critical to the research. Once the researcher identifies the research problem, Erlandson et al., (1993, p. 53) state that "the researcher is compelled to identify a site that maximises the opportunity to engage in that problem". The sampling of cases is an important aspect of any type of research approach, especially when building theory from case organisations. Patton (1990) contends that the logic underlying the sampling approach constitutes a fundamental difference between qualitative and quantitative research. Therefore, a purposeful sampling plan should be followed (Patton, 1990) where case studies are chosen (Eisenhardt, 1989), where a small number of cases are selected on the basis of the information richness, from the narratives collected, will provide. Patton (1990) purposed a number of purposeful sampling strategies all based on variations of the same assumption of purposiveness. One plan must be selected, on the basis of the objective of the research, as all of the different strategies cannot be pursued simultaneously. In the case of this investigation, three dimensions concern the selection of sampling must be isolated. The dimensions are as follows:

The ***first*** dimension concerns the structure of the organisations selected. The IS Security function must be separate from the IT department to ensure that the case selected prioritises the process and follows basic guidelines from industry and academia (Dutta & McCrohan, 2002) at a corporate level (Section 3.5.1, Step 3 of the CSP).

The ***second*** dimension of sampling applies to the utilisation of a KM strategy in a CS function within the selected organisations. Support functions are identified in the literature as knowledge-intensive environments which effectively operate as silos (Huang et al., 2007) within organisations. Support functions predominately apply a form of a KM initiative in supporting an organisations customer base (Becerra-Fernandez, et al., 2004). Therefore this dimension would provide a KM initiative from which to learn from and benchmark against the approaches used in the ISS functions. Due to the silo nature of CS functions, the impact of IS Security on the technologies, people and processes used to manage the technical knowledge required within these closed support environments can be easily identified to answer research question three.

CS and IS Security functions should collaborate in identifying risks to KM and should be cognisant of the IS Security and control applications available in the KM environment (Jamieson & Handzic, 2004). Therefore CS functions operate closely with IS Security functions for support and engineering for product expertise (Section 3.5.1, Step 2 of the CSP).

The *third* dimension of sampling applies to the selection of the different cases or the different organisational settings in which the three research questions are going to be researched. The sampling method utilised relied on the intensity and criterion sampling strategies (Patton, 1990). Intensity sampling required the selection of only organisations of a certain size, and complexity were considered to ensure that they would feature separate ISS and CS functions, operate on a global scale and in a knowledge-intensive, competitive business environment. This also ensured that the ISS functions had to be also developed to a certain degree so that informants could be identified in these functional areas. Criterion sampling meant that the organisations had to operate in different industries so that the findings would have a wider domain of applicability. However opportunistic sampling was also necessary as the researcher tried to secure access that would allow for proper data collection by selecting organisations where a friendly sponsor could be found and used as an informant.

In addition to the issue of purposive sampling the issue of sample size was considered. Sample size does not have to follow the rules of probabilistic sampling as no claim is made that the cases selected are statistically representative of a population (Patton, 1990). Lincoln and Guba (1985) argued for a more specific criterion to determine when a suitable sample size has been reached. Lincoln and Guba (1985) suggested that the termination of a study is determined by its informational needs. Essentially this is achieved when no new information is uncovered in additional case organisations and the additional data collected becomes redundant, then the sample size can be considered to be sufficient. This is therefore negotiated between the researcher and the relevant stakeholders of the research as the project unfolds and the findings emerge. However an overall control mechanism must also be put in place in order to monitor the progress of the research as such a loose criterion for the termination of the field work could potentially lead to an on-going study covering many years of investigation.

The researcher visited a number of organisations to verify their suitability, and if suitable, gained official confirmation of management's commitment to the study. The criterion presented led the researcher to exclude the following five case organisations.

1. University College Cork is one of the colleges which make up the National University of Ireland (NUI), the largest university in Ireland. This case was initially approached due to its size and the insistence of key informants that ISS was a separate entity in the structure of the university. However, ISS was fully immersed in the IS department and some individual academic departments utilised their own IT group which was separate from the university's department.

2. FMC Corporation is a U.S. chemical manufacturing company with over five thousand employees. Preliminary interviews determined that ISS was not separated from the IT department and that interviewees (eight in total) did not manage knowledge but data.

3. ESB Group is a multinational with its headquarters in Dublin, Ireland. The company was of sufficient size and separated ISS from IT five years before this research began. However, despite assurances to the contrary, a CS function utilising KM initiative was not evident. The ESB group was just beginning to investigate the possibility of using KM to improve internal CS processes and expected the researcher to guide the implementation of a KM strategy. While a KM audit report was supplied to the organisation, the case was not suitable to investigate how ISS could leverage the concept of KM as it was not yet developed internally.

4. Musgraves is Ireland's leading Cash and Carry company. This case was initially interesting as it had experienced enormous growth in the years prior to the study. However the case did not, despite assurances by the primary informant, manage knowledge.

5. SERV-Co provides outsourcing capabilities to some of the world's leading technology companies such as Dell. It was initially targeted as it utilised a KM initiative as part of its strategy in supporting customer needs. It also had a large IS department spread across its subsidiaries. While the case was not suitable for the research objective it was suitable as a pilot case study to help the researcher clarify the dimensions of variables (Davila, 2000) and refine the different research approach methods.

The factors presented above led the researcher to select the following two case organisations:

1. CME-Co is a technology company and a world leader in products, services, and solutions for information storage and management. CME-Co has subsidiaries located throughout the world with its headquarters based in Hopkinton, MA and its main European manufacturing centre in Cork, Ireland. The organisation has separate ISS and CS functions. The CS function also has an established KM initiative.

2. TELE-Co is an American multinational, Fortune 100, Telecommunications Company. It is a manufacturer of wireless network infrastructure equipment with fifty-three thousand employees. The organisation has separate ISS and CS functions. The CS function also has an established KM initiative.

The two multinational organisations were chosen to investigate how IS Security could leverage the concept of KM. The two cases were categorised as engineering and technological organisations. CME-Co operates in the storage sector and TELE-Co in the telecommunications sector. The portfolios of the two case organisations are wide and complex requiring significant expertise in supporting customer needs. This strategy facilitated Darke et al., (1998) belief in studying a phenomenon in diverse settings. Additionally due to the nature of the environment that the organisations operate in they are subject to rapid technological advances, regulatory constraints and environmental threats such as reverse-engineering and negative security incidents which impact the operations of the organisations. After these visits, the researcher was satisfied that a viable research relationship had been established with the two organisations. The selection process was dependent on getting access to the organisations. Given the topic the researcher initially found it extremely difficult to gain access to appropriate cases despite the assurances of confidentiality and of the benefits of participating in such a

study. The two organisations which did participate saw the benefits from both an IS Security and KM perspective. The following section discusses the justification of investigating the objective of the study within the IS Security and Customer Support functions of the multinationals identified.

3.3.2.1 Units of Analysis: the Customer Support and IS Security Functions

The Customer Support and IS Security functions which service (internal and external) customers are strategic functions within Engineering organisations. The firms selected provided rich context to the study (Step 1 of the case study protocol). In the context of this investigation, the embedded units of analysis (Yin, 1989) chosen for inclusion in each case were the organisational Customer Support and IS Security functions (Steps 2 and 3 of the CSP).

In exploring what each CS function did in adopting a KM approach the researcher will be able to determine if the approach was successful in deriving functional and organisational benefits. Support functions are structured to operate as separate business functions in order to support customers of the organisation. The functions were identified to investigate the implications of IS Security on the technologies, people and processes used to manage the knowledge required within closed support environments. CS and IS Security functions should collaborate in identifying risks to KM and should be cognisant of the IS Security and control applications available in the KM environments (Jamieson & Handzic, 2004). Each study organisation has invested heavily in a Customer Support function/unit to support the corporate business units or organisation's customers as it is seen as a value added task of the umbrella organisation. The focus of the study is the IS Security functions within each case. These functions perform a myriad of tasks such as securing the validity of information/knowledge through to alignment of technical controls (access controls, identity management) to resources. The function facilitates control structures and processes. Additionally, the function must support business strategies and align the necessary controls (technical, formal and informal) to business activities.

Each of the factors identified in Figure 2.5 required attention in systematically mapping the practitioners, processes and technology used in the management of function specific knowledge. In exploring what each Customer Support function did in managing knowledge the researcher can determine if the approach was successful in deriving functional and organisational benefits. Figure 3.1 illustrates and Section 3.5 explains in detail the research protocol used in this study to explore the embedded units of analysis.

3.3.3 Data Collection Techniques

The data gathering techniques used for case studies are numerous. They range from personal interviews and questionnaires to document analysis (Galliers & Land, 1987). The first step in research is to choose the research approach; the next is to select the technique used to gather the information on the phenomenon under investigation. Literature dictates that the technique chosen should reflect the objective of the study (Robson, 1993). The two primary techniques for case study are interviews and document analysis (Marshall & Rossman, 1989). Table 3.5 outlines the various strengths and weaknesses associated with the different data gathering techniques (Yin, 1994); to offset any limitations multiple methods were employed. For the purpose of this research the researcher selected the following data gathering techniques: structured and personal interviews, document analysis, and coding (open, axial, and selective). The

primary source of qualitative research data collected was from interviews. In fact Walsham (1995, p.78) contends that interpretive studies rely on interviews, as "…it is through this method that the researcher can best access the interpretations that participants have regarding the actions and events which have or are taking place, and the views and aspirations of themselves and other participants". Numerous researchers in the IS field report the employment of semi-structured interviews as the primary source and method of choice (Orlikowski, 1993; Butler & Fitzgerald, 2001) with document analysis and web pages as secondary sources (Marshall & Rossman, 1989).

3.3.3.1 Semi-Structured Interviews

Interviews are frequently used as a data collection technique for qualitative research in the IS field (Marshall and Rossman, 1989) and as "an essential source of case study information" (Yin, 1984). An interview can be described simply as a conversation, the purpose of which is to acquire valid and reliable information (Marshall & Rossman, 1989; Robson, 1993). There are a number of different types of interviews that are based on the degree of structure of the interview, and which can be represented on a continuum from structured to unstructured (Fontana & Frey, 1994). A structured interview utilises a predetermined set of questions and records the responses using a standard set of response categories (Fontana & Frey, 1994), while an unstructured interview allows the researcher to probe more deeply to obtain information that may not have been immediately obvious. The semi-structured interview, on the other hand, utilises a set of loosely structured, flexible questions which can be adapted to facilitate the context and flow of the interview (Stone, 1978). This enables the researcher to explore more deeply issues that are considered important and enables the respondent to highlight important issues that the researcher may have excluded in error (Remenyi & Williams, 1995). The adoption of interviews as a data collection technique provides a number of advantages to the research approach. They enable large amounts of comprehensive and contextual data to be collected quickly (Marshall & Rossman, 1989). They are flexible and adaptable facilitating the use of immediate follow-up questions for data clarification and omissions (Marshall & Rossman, 1989). They also facilitate data collection in a natural setting and as a result maintain the complexity of the phenomenon being studied (Benbasat et al., 1987; Galliers, 1993; Robson, 1993). The interview methodology is based on the belief that it is possible to investigate a phenomenon by merely asking people to talk. This ability to digress from the standard interview protocol allowed the researcher to explore issues which arose during the conversation irrespective of the case or function.

Erlandson et al., (1993, p. 86) state that "…the semi-structured interview is guided by a set of basic questions and issues to be explored, but neither the exact wording nor order of questions is predetermined". The interview guide is basically a checklist to ensure that all of the relevant topics are discussed (Patton, 1990). The interview guide (Appendix B) used a combination of focused and open-ended questions. In each organisation an informant from each function was identified who helped in validating the findings and the emergent concepts. This was a particularly useful approach in assessing the matrices created to categorise the different roles of IS Security and Customer Support knowledge in the two functions. Additionally informants were identified who helped to assess data relevant to the organisational infrastructure of each case. Identifying and selecting an informant was guided by Gibson's (1960) "...it does not mean that the man with inside knowledge has evidence for his conclusions ...but [that] he is in a...favourable position to accumulate evidence".

3.3.3.2 Roles and Responsibilities

Within this research study the interviews were conducted on site varying from one to a three hour time frame (Table 3.3). Each interviewee gave permission for the conversations to be recorded and when requested, the Dictaphone was switched off and field notes were made (Walsham, 1995). Each interviewee was identified according to their "expertise" in either field in addition to their role as, for example, the Customer Support manager might be the knowledge champion within one case or the strategy might be championed by the human resource manager in another. The IT manager and function can also play a significant part in IS Security. These factors enabled the researcher to focus on the appropriate issues applicable to each function within the subsidiary and members who are geographically dispersed but still a part of either function (section 3.5.1). Following the first round of interviews, transcripts were sent to the informants for review and verification of the content. ISS and CS informants were also selected to review the display matrices created. Table 3.3 outlines the roles and responsibilities of each interviewee in the two case organisations as well as the pilot case study. Details regarding the interviewees years in service, allocated function and the duration of each interview are also provided. Furthermore, the personnel interviewed were the key decision-makers and most knowledgeable practitioners, in relation to the ISS and CS functions. Supplemental informants such as HR managers and former employees were interviewed to explain the organisational infrastructures and verify the data collected from the primary informants.

3.3.3.3 Document Analysis

Document analysis (Marshall & Rossman, 1989) is a useful data gathering technique. This technique is vital for collecting in-depth information regarding processes, which may not be recalled in interviews and postal questionnaires. The researcher reviewed information about the existing IS Security policies, departmental information and corporate policies regarding KM. The value of the findings gathered through semi-structured interviews can also be increased through the use of this technique as the researcher's understanding of the business processes would be greater. Documentation review provides the researcher with more insight into the background of the case (Marshall & Rossman, 1989). The researcher deemed it appropriate to use this technique to gather information

However, retrievability and access to documentation can be slow and can reflect the reporting biases of the authors. Within this research study, this source of data was exploited as much as possible. The documentation collected in each case organisation provided specific details to corroborate, and in some instances clarify, factual evidence collected through interviews. Table 3.4 presents a list of the documentation collected and examined for each case organisation. Tables 4.1 (SERV-Co), 5.1 (CME-Co) and 6.1 (TELE-Co) provide summarised profiles of the pilot case study and the two case organisations. Tables 5.2 and 6.2 were derived from analysing the documentation collected from CME-Co and TELE-Co and combining it with the roles and responsibilities of the interviewees to provide an overview of the data gathered from multiple sources within the two case organisations. These tables were created from examining the documentation presented in Table 3.4. The documentation collected was also used to collaborate and verify the types, reservoirs and knowledge processes identified from the data collected (Tables 5.3: 5.12 and 6.3: 6.12).

ROLES AND RESPONSIBILITIES																			
IS SECURITY FUNCTIONS					Interviews		CUSTOMER SUPPORT FUNCTIONS				Interviews				Interviews				
	Region	Role	ISS Expertise	Years	No	Hrs	Region	Role	CS Expertise	Years	No	Hrs	Other	Years	No	Hrs
CMECO	Cork	IT Manager	IT Services/ISS/SOX/Business	8	1	1.5	Cork	CSC Customer Mgr	Eng/Prj Mgt/Product Portfolio	12	1	1.5	Purchasing Mgr	12	1	1
	Cork	Security Coordinator	Controls/Regs/Practices/Standards	4	3	2.5	Cork	KMS Engineer Trainer	Eng/KMS/KM Trainer	10	3	3	Project Manager	7	2	1
	Cork	Remote Access	Network Security/Controls/Risks	10	1	1	Cork	KDG Officer	Eng Concepts/Learning Skills/KM	2	1	1	6th Sigma			
	Australia	Security Coordinator	Controls/Regs/Practices/Standards	5	1	2	U.S.	Engineering Trainer	Eng/KMS/KM Trainer	4	1	1	Operations Mgr	11	1	1
	U.S.	Security Coordinator	Controls/Regs/Practices/Standards	10	2	2	U.S.	KMS & DB Admin.	ACL/DB Development	8	1	1	Former IT Mgr	5	0.5	3
	Cork	Infrastructure Manager	Interoperability	11	1	1	Cork	Tech Eng Level 1	Eng. Product Portfolio	2	1	2				
	U.S.	OIS/KM Coordinator	Regs/Practices/methods/Standards	2	1	3	Cork	Tech Eng Level 2	Eng. Product Portfolio	5	1	1				
	U.S.	Remote Access	Network Security/Controls/Risks	10	1	1	U.S.	Knowledge Consultant	Eng/Modelling/Tech KM/KM	14	2	2				
	U.S.	Corporate Sec Officer	Compliance Expert	7	1	2	U.S.	Engineer Mgr	Eng/Prj Mgt/Product Portfolio	13	1	2				
	U.S.	GIS Director - by Email	ISS Metrics, SOX	12	0	1	Cork	E-Services	Encryption/VPN/SSL/Risk	8	1	2				
	Total:	Avg Years:- 3 Groups::	8		12	17					20	185			4.5	6
	Region	Role	ISS Expertise	Years	No	Hrs		Role	CS Expertise	Years	No	Hrs	Other	Years	No	Hrs
TELECO	EMEA	IT Manager	IT Services/All Aspects-ISS	9	2	2	EMEA	Engineering CS	Eng Product Portfolio	12	1	1	Director of HR	6	1	1
	U.S.	MGS Coordinator	Infrastructure/Tools/Reg Bodies	7	1	1	Cork	CS Eng. Manager	Eng Product Portfolio	10	1	2	Former Eng. Mgr	15	2	2
	Cork	Security Officer	Controls/Regs/Practices/Standards	3	3	2	U.S.	Design Engineer 1	Eng Product Portfolio/Quality/PKM	5	1	1	Former Prj Mgr	7	1	0.5
	U.S.	Security Officer	Network Security	4	1	1	U.S.	Design Engineer 2	Eng Product Portfolio/Quality/PKM	7	1	1				
	U.S.	Corp Sec Coordinator	All ISS, SOX, Business	8	1	1	U.S.	Design Engineer 3	Eng Product Portfolio/Quality/PKM	3	1	1				
	U.S.	TIP Auditor	Reg Info Modelling, ISS	2	1	1	U.S.	Design Engineer 4	PKM Coordinator	7	1	2				
	U.S.	Security Officer	ID Scanning/ACL	1	1	2	U.S.	DB Analyst	Content Mgt. System / All DBs	9	1	1				
	U.S.	TIP Coordinator	Auditing/Regs/Patches External K	5	1	1										
	U.S.	Compliance Coordinator	Regulations	4	1	2										
	Total:	Avg Years:- 3 Groups::	5		12	15					7	9			4	3.5
SERVCO : PILOT CASE STUDY																
	Region	Role	ISS Expertise	Years	No	Hrs	Region	Role	CS Expertise	Years	No	Hrs	Other	Years	No	Hrs
SERVCO	U.S.	GIS Manager	IT/All Aspects-ISS/ITIL/ISO1799	12	1	1	Cork	CS Manager	IT Services/Best Practices/SDLC	4	1	2	Director of HR	10	1	1
	U.S.	Security Officer /Analyst	Controls/Regs/Assessments	4	1	2	U.S.	Engineering CS	Eng Product Portfolio/SDLC	3	1	2	Matrix Trainer	4	1	1.5
	Cork	Security Officer 1	Controls/Regs/Practices/Standards	7	1	1	U.S.	ERP Analyst	ERP/DB Implementation	8	1	1				
	U.S.	Security Officer 2	Controls/Regs/Practices/Standards	2	1	1	U.S.	Senior QA Engineer	SDLC/Customer Requirements/SOX	2	1	1				
	U.S.	Infrastructure Manager	Access Control/ITIL/Systems	2	1	1										
	U.S.	Compliance Coordinator	SOX/Best Practices, Methods	4	1	1	U.S.	Proj. Leader	SDLC/KMS/IT Requirements	5	3	3				
	Cork	Access ITIL Manager	Access Control/ITIL/Seg of Duties	3	1	2	U.S.	Business Analyst	Market/Customer Req/SDLC	7	1	1				
	Cork	Help Desk Manager	Access Control/ITIL/Seg of Duties	6	1	1	Cork	SDLC Coordinator	Quality Control/Methods/Sec.	2	2	2				
	U.S.	DB Administrator	ACL/SDLC/DB Development	8	1	0.5										
	Total:	Avg Years:- 3 Groups::	5		9	10.5					10	12			2	2.5

Table 3.3: Roles and Responsibilities of the Interviewees

Case	DOCUMENTATION ANALYSED	
CME-Co	Annual Reports: 2001/2005/2006/2007 | Corporate Newsletters: CME-Co Profits Soar by 20% on Storage Demand Presentations: CME-Co Review 2007 and Compliant ILM Strategy	
	Security Documentation: • CME-Co Customised – ISO17799 Documentation • Security Policies Re: email/ Internet/ Remote • Data Centre - Disaster Recovery Procedures[3] • Business Continuity Procedures • Intranet: OISRM Website / IS Department • CME-Co Website – www.CME-Co.com	**Customer Support Documentation:** • Primus (CBR Tool) White paper • ILM[4] White paper • Power-Link & Knowledge link White paper • KCS[5] White paper • Viewed: Primus CS View| Power-Link: Extranet • Intranet: Customer Services Website
TELE-Co	TELE-Co Website – www.TELE-Co.com	
	Security Documentation: • TELE-Co ISO17799 • TELE-Co Standard Operating Procedures http://cfr.corp.TELE-Co.com/sops/SOP/ • Standards of Internal Control (SIC) • Electronic Information Security Standards (EISS) http://internalcontrols.TELE-Co.com/ic/ca/SIC/	**Customer Support Documentation:** • KM Courses @ TELE-Co University • Six Sigma[6]: A Necessary Change • M-Gates[7] White Papers / K-Gates • Intranet: Customer Services Website • University – Online Courses: Six Sigma, M-Gates
SERV-Co: *Pilot	• SERV-Co Website – www.SERV-Co.com /Annual Report 2006/07, SERV-Co PR Pack / Organisation Chart	
	Security Documentation: • Customised: ISO17799, ITIL & Sec-SDLC[8] Guidelines, SDLC[9] Template • Security Policies: Re: Segregation of Duties, email, Internet, Remote Access, Corporate Policy Business Continuity[10] Procedures • Viewed: iViewXT ISS View/ Help Desk System	**Customer Support Documentation:** • Presentations: iViewXT Customer Presentation • iViewXT White Paper • Viewed: iViewXT CS View/ Customer View • Intranet: Customer Services (GIS) Website • JD Edwards (ERP)[11] User Manual

Table 3.4: Case Documentation Analysed.

[3] Disaster Recovery Procedures (DRP) is most common mitigation procedure used to recover from a disaster such as a power outage and forced shutdown of corporate systems.
[4] ILM (Information lifecycle management) is an IT strategy. It's based on the fact that the value of information changes for an organisation. That is information requires different levels of accessibility and protection.
[5] Knowledge-Centred Support (KCS) is a KM strategy developed by the Primus vendors. KCS practices involve collaborating, sharing, using and improving knowledge. KCS incorporates the process of creating a solution in Primus to the evolution of that solution when used by other engineers.
[6] Six Sigma was developed to systematically improve processes by eliminating defects.
[7] M-Gates framework is a high-level process based on the Stage-Gate Process. It represents a comprehensive set of Marketing, Engineering, Project Management and Manufacturing activities to ensure proper business planning and execution.
[8] SecSDLC implementation is accomplished through changing the configuration and operation of the SDLC to incorporate security into the traditional SDLC.
[9] SDLC is a development methodology which incorporates the following phases: (1) Feasibility Study, (2) Systems Investigation, (3) Systems Analysis, (4) Systems Design, (5) Implementation, (6) Review and Maintenance.
[10] Business Continuity Procedures (BCP) encompasses continuation of business activities if catastrophic event occurs.
[11] JD Edwards (JDE) is a software company which sells Enterprise Resource Planning (ERP) solutions.

3.3.4 Limitations Associated with the Methods

The literature provided a lens to identify gaps which existed in both the IS Security and KM domains. The researcher wanted to avoid repeated or expected investigations, for example the impact of technologies on IS Security and KM, to facilitate theory creation and contribute to both the IS field and relevant communities of practice. Therefore "…choosing the right literature in tandem with doing analysis one can learn much about the broader and narrower conditions that influence a phenomenon. However, any categories, hypotheses and so forth, generated by the literature have to be checked out against real (primary) data", (Strauss & Corbin, 1990, p.55). This interplay advocated by Strauss and Corbin (1990) is beneficial in producing rich theory and is adopted for this research study. The conclusion drawn by the researcher upon reviewing literature in both domains was that it has not evolved to identify how IS Security can leverage the concept of KM. The researcher investigated the phenomenon with no prior hypothesis and explored it to deepen the IS fields and practitioner understanding of the role that it plays within organisations and the impact of one on the other. The limitations of the selected research strategy for this study are the problems associated with the use of interviews, and document analysis.

EVIDENCE	STRENGTHS	WEAKNESSES
Documentation	Stable :repeated review Unobtrusive: exists prior to case study Exact: names etc. Broad coverage: extended time span	Retrievability: difficult Biased selectivity Reporting bias :reflects author bias Access: may be blocked
Archival Records	Precise and quantitative	Privacy might inhibit access
Interviews	Targeted: focuses on case study topic Insightful: provides perceived causal inferences	Bias due to poor questions Response bias Incomplete recollection Reflexivity: interviewee expresses what interviewer wants to hear
Direct Observation	Reality: covers events in real time Contextual: covers event context	Time-consuming Selectivity: might miss facts Reflexivity: observer might cause change Cost: observers need time
Observation	Insightful into interpersonal behaviour	Bias due to investigator's actions
Physical Artefacts	Insightful into cultural features Insightful into technical operations	Selectivity Availability

Table 3.5: Strengths and Weaknesses of Data Collection Techniques (Source: Yin, 1994).

Table 3.5 illustrates the strengths and weaknesses of each component of the research strategy. While there are strong arguments against the use of qualitative research (Walsham, 1993) it provides the researcher with in-depth rich data. Corporate documentation is created for a specific audience and for a specific reason, for example shareholders are provided with a different perspective on the organisation they have invested in from that given to the employees. CME-Co used their Intranet to promote the company internally and instil in the employees a sense of team and corporate competition. The greatest weakness of this data gathering technique is reliability (Yin, 1984; Remenyi, 1998). Document analysis is important in analysing the problem situation; the pluralistic approach was adopted to reduce the impact of the weaknesses of this technique. Section 3.4 discusses the data analysis approach used.

3.4 Data Analysis

This section discusses the approach used for the data analysis stage of this research. The data analysis phase enables theories and themes to emerge from the study (Erlandson et al., 1993). Marshall and Rossman (1989, p.12) describe the practice as:

> "…the process of bringing order, structure, and meaning to the mass of collected data. It is a messy, ambiguous, time-consuming, creative, and fascinating process. It does not proceed in a linear fashion; it is not neat. Qualitative data analysis is a search for general statements about relationships among categories of data; it builds on grounded theory".

The result of this process is the collection of rich data that will generate a rich hypothesis. The literature enabled the researcher to identify the topic and this section begins by discussing how the literatures informed the theory building phase.

The activity of data reduction refers to the method of selecting, focusing, simplifying, abstracting, and transforming the data that appears in transcriptions (Miles & Huberman, 1994). Miles and Huberman (1994) argue that "anticipatory" data reduction can occur before data is even collected. In relation to this research study anticipatory data reduction began with the development of research questions and then choosing which data collection technique to use. By carefully selecting only a specific number of interviewees the amount of data that is collected is reduced (Table 3.3). Data reduction also serves to "condense" (Tesch, 1990) the data that is collected and as a result can organise, sharpen, and focus the conclusions that are drawn from the research study (Miles & Huberman, 1994).

Next the task of listening to and transcribing the taped interviews, which was a long process, was undertaken. NVivo, a database for storing, parsing, categorising, and querying text files was recommended as a possible software package. Transcripts are copied into NVivo, as the transcripts are read passages are marked as 'nodes', a term used by the software, where they are identified as describing themes recognised from the literature review. Other passages are identified and marked up as describing other themes that a researcher interprets as being raised by the interviewees as important. This process is supposed to enable easy access to the data that is attributed to any particular theme. However after approaching four colleagues who had used NVivo, and other similar packages, the researcher decided not to use a software package for analyses. None of users would recommend the software packages used and stated that there was little added value from the use of software.

Manual transcribing enabled the researcher to analyse the data before coding and comparatively analysing it. Coding was used as a method to organise and condense the data collected from interviews and facilitate the drawing of conclusions (Miles & Huberman, 1994). Additionally the Miles and Huberman (1994) matrix displays were ideally suited to the organisation and analysis of patterns in the data collected across two case organisations (Lillis & Mundy, 2005). The matrix displays offered a means of identifying themes in the data, categorising them, quantifying their regularity and representing this analysis in diagrams or additional display matrices. The displays enabled the researcher to produce an audit trail for the evaluation of rigor and extend the process by which conclusions are drawn.

Finally, while the framework illustrated in Figure 2.5 and discussed in section 3.1 of this Chapter grounded this study, it allowed for sufficient scope to enable additional variables to emerge from the contextual settings of the two organisational environments and pilot study participating in this study. Prior theory informed the use of the data collection and analysis techniques used. However the researcher deemed the use of a pilot study as an integral part of testing the research protocol and interview guide in order to refine the data collection and analysis techniques as well as to familiarise the researcher with the phenomenon itself (Yin, 1994).

3.4.1 Pilot Case Study

The literature has always recognised the value of refining methods for case study research, for example, pilot case studies which clarify the dimensions of variables or potential inter-relationships (Davila, 2000) or validate, for example literature, findings (Widener & Selto, 1999) are recognised approaches in refining methods. Researchers can learn a great deal from conducting a pilot case study. Pilots are extremely useful steps in investigating a phenomenon (Lillis & Mundy, 2005) they can result in changes to the different data collection and analysis tools used as well as the research protocol applied. However it is important to remember that a pilot case study is only the first step in the theory-building process of case study research. Chapter 4 applied the research protocol developed and described in this Chapter to the pilot case study.

3.4.2 With-in Case Analysis

Within case analysis involves detailed write-ups of case descriptions to generate insight (Eisenhardt, 1989; Miles & Huberman, 1994). These rich descriptions provide researchers with the ability to understand the context of the phenomena under study. As explained by Eisenhardt (1989), there is no standard format for this type of analysis and a variety of approaches can be utilised and manipulated by researchers. Cases have been developed by academics as introductions to theoretical work through the compilation of organisation case histories, descriptions which are compiled through the use of taped transcripts and tabular displays (Miles & Huberman, 1994). As described by Brown (2000, p.46), case narratives are "…the most useful way to understand sense-making". The narrative, in the context of this study provides a frame of reference to fully understand and report the accounts of the different informants within and across the different IS Security and CS functions and their approaches to managing knowledge. Additionally, these (informant) accounts are triangulated with available documentation (Table 3.4) to ensure that the case is reported accurately. Some researchers regard narratives as messy and uncodeable data, yet the insights they provide are invaluable. The research lens described in sections 2.7.1 and 3.1 was used in this study to provide structure to the investigation. The lens enabled the researcher to make sense of the phenomenon under analysis.

For example, in Chapters four, five and six each case and pilot study has been analysed and structured according to the case study protocol (CSP) described in section 3.5. The backgrounds and organisational infrastructures of the two cases were presented. The investigation of the two case studies has provided rich contextual descriptions of the IS Security and CS functions. The types and reservoirs of Knowledge used by the two functions operating within the cases were described. The approaches used in managing this knowledge are also discussed in detail. Finally the two functions KM approaches,

mechanism used and impacts were compared and contrasted. Therefore the within case analysis provides insight into the phenomenon under investigation.

3.4.3 Cross-Case Analysis

Research shows that knowledge is communicated effectively through a convincing narrative that is delivered with formal elegance and passion. As with the case narratives used in Chapters five and six, there are various strategies available in searching for cross–case patterns, for example: select categories, within–function similarities, differences (Bourgeois & Eisenhardt, 1988; Gersick, 1988) and display matrices to compare several categories simultaneously (Miles & Huberman, 1994). Each of these tactics can be combined to draw out more concrete theoretical insight. Chapter seven of this study presents the cross-case analysis. It was used to progress from the within case analyses conducted in Chapters five and six and analyse the findings from the two case organisations to address the research questions. The Chapter consists of three sections, each addressing one of the three research questions outlined in section 3.1.3. The purpose of this Chapter is to combine the findings from the three questions and address the objective of this study.

3.4.4 Data Collection, Analysis and Time Line

The timeline for this investigation is outlined in this subsection and the steps taken are illustrated in Figure 3.1. The diagram illustrates the six steps completed in order to answer the research objective and questions (section 3.1), for this study. This study was initially focussed on IS Security and a change requiring the incorporation of knowledge management was made in October 2006. As a result the current literature review and research strategy design which were originally completed in September 2005 and were subsequently updated in July 2009. Additionally, the data collected, analysed and write-ups for four case studies were deemed irrelevant for the current objectives and additional cases were sourced and investigated. The current research objective and propositions were investigated in a pilot case study in June 2007, which ultimately did not meet the case selection criteria, as outlined, in section 3.3.2. However the pilot case study did allow the researcher to test the research lens (Figure 2.5) and case study protocol (Figure 3.1). The data was collected through semi structured interviews and documentation in the two case study organisations over a six month period from July to October 2007. Transcribing, coding and analysis for the within case write-ups took between six and eight months for CME-Co and TELE-Co respectively. The cross-case analysis took three months and was completed by June 2009.

Section 3.5 summarises Chapter three and describes the case study protocol (CSP) used for this study. Finally section 3.6 concludes this Chapter.

3.5 Summary and Case Study Protocol (CSP) for this Research Study

The objective of this study is to explore how Information Systems Security (ISS) could leverage the concept of Knowledge Management (KM) in the context of two multinationals. The selection of the most appropriate approach is a key enabler of any investigation. The selection must be based on the research objective and the nature of the study. Due to the exploratory nature of the study an interpretative strategy was adopted utilising a combination of research methods and techniques such as two-case

studies and pilot case study, semi-structured interviews and document analysis. In terms of expected findings, given the gaps which exist in both the KM and IS Security literatures where a relationship between both fields has rarely if ever been identified, the IS field has been neglectful of this strategic and vital phenomenon. Previous studies have been insufficient in investigating IS Security as few if any studies utilise a qualitative approach and therefore eliminating holistic, in-depth rich descriptions of core issues within the field. IS Security approaches have been grounded in positivism. An investigation exploring how IS Security could leverage the concept of KM should provide rich data and aid the researcher in exploring the phenomenon. Section 3.5.1 describes the operationalisation of the research strategy outlined and discussed in this Chapter.

3.5.1 Research Protocol and Steps

The researcher used a specific research protocol which was followed throughout the investigation to build an integrated map of the research objective from a pilot study and two case studies and across the two case organisations. The protocol followed is outlined in a series of six steps (Figure 3.1) four of which are replicated in each case organisation and as far as step three in the pilot case study:

Step 1: Study the Organisational Infrastructure

This step provides the context to the study, to understand the environment in which the functions under analysis operate. An organisation and its subsidiaries are composed of a series of information/knowledge handling activities coordinated through the establishment of rules, policies and procedures all of which must be understood. Additionally, the culture, structure and (threats from) the environment in which the organisation operates contributes to its overall IS Security and KM profile. The structure of the organisation strongly influences core activities and the level of engagement with which these are consistent with the enterprise's goals (business drivers). It is composed of organisation charts, ethical codes and job descriptions. Therefore, appreciating the role of senior management (Corporate, KM and IS Security governance) helps to ascertain if the organisational structure is supportive of the exploitation of IS Security-related and KM initiatives. It is through answering RQ1 that the researcher can fully appreciate the context in which the objects under investigation operate and the influence of the structure, culture, management and business environment (for example regulations) of the organisation. Additionally while the focus of the research is primarily focused on a single type of informant – the IT professional – the bias identified by Lee et al., (1991) is removed by the use of multiple types of informants (Table 3.3) relevant to the research objective.

Step 2: Study Customer Support Function

Step 2 establishes the justification for undertaking a function specific analysis to identify the context of the support function. In exploring what each Customer Support (CS) function did in adopting a KM approach the researcher can determine if the approach was successful in deriving functional and organisational benefits, the conclusion of which is derived in the context of this research. Customer Support functions are structured to operate as separate business functions in order to support customers of the organisation. The functions were identified to investigate the

implications of IS Security on the technologies, people and processes used to manage the technical knowledge required within closed support environments. CS and IS Security functions should collaborate in identifying risks to KM and should be cognisant of the IS Security and control applications available in the KM environment (Jamieson & Handzic, 2004). Therefore CS functions operate closely with IS Security functions for support and engineering for product expertise. Each study organisation has invested heavily in a Customer Support function/unit to support the corporate business units or customers as it is seen as a value added task of the umbrella organisation.

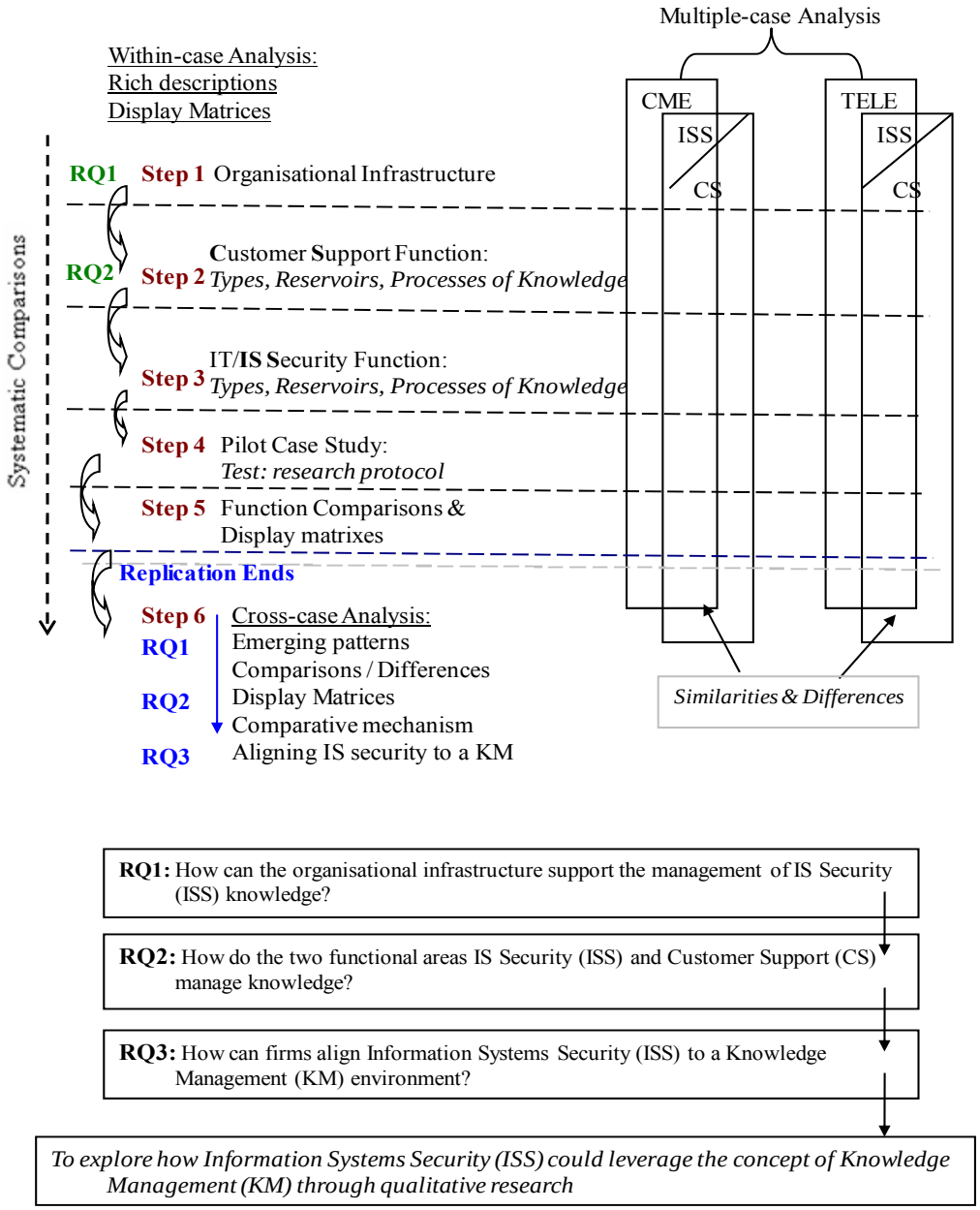

Figure 3.1: Research Protocol and Research Steps.

Step 3: Study Information Systems Security Function

The focus of the study is the IS Security functions within each case. These functions perform a myriad of tasks such as securing the validity of information/knowledge through to alignment of technical controls (access controls, identity management) to resources. The function facilitates control structures and processes. Additionally, the function must support business strategies and align the necessary controls (technical, formal and informal) to business activities. If there is an absence of "…an individual or section that is solely accountable for security issues, then the deployment of activities related to security may be slow, hampered or futile" (Dutta & McCrohan 2002, p. 76). It is through answering RQ2 that the researcher has identified the people, processes and technologies used in the function's attempt to manage information and IS Security knowledge pertaining to the case's IS Security landscape. Evidence from the within case analysis illustrates how IS/Security personnel interoperate. Therefore, it is vital to understand the function's role within the cases and identify the people, processes and technology used to protect the corporate boundaries. As already stated, the rich description (collected through Steps 2 and 3) used to answer RQ2 enables the researcher to compare the cases systematically and identify the different research categories. The research model developed from an analysis of the literature review (Figure 2.5) has informed the mapping of the different types and reservoirs of knowledge within the cases while additionally systematically mapping the people, processes and technology used in its management.

Step 4: The Pilot Case Study

The pilot case study establishes the validity of the different data collection and analysis techniques as well as testing the case study protocol (CSP). Therefore the pilot case study was used to refine the different methods used and to clarify the potential relationships between the variables identified in the literature review (Chapter 2). Steps 1, 2 and 3 were undertaken to determine if they were of value in addressing research questions one and two. The pilot was also used to allow the researcher to become familiar with the phenomenon.

Step 5: Approaches Used to Manage Knowledge

Within-case analysis requires detailed case study write-ups for pure descriptions and the generation of insight of the objects under investigation (Gersick, 1988; Eisenhardt, 1989). A constructive description will provide a common frame of reference in order to better recognise, understand and ultimately structure the rich accounts provided by the informants. Chapters five and six have a description of the organisation's background, the IS Security and CS functions, and employ supplemental informants such as HR managers to explain the organisational infrastructures. Additionally, the accounts were triangulated with available documentation to further the findings.

In the context of a case study, descriptions are tools which can provide a suitable structure to answer the research questions and act as a blueprint to predict future organisational behaviour. Matrices are used by the researcher to display the different types and locations of knowledge used by the two functions and the approaches used to

manage function specific knowledge. This step also involved explaining the relationships between CS and the IS Security functions. An analysis of the contrasting approaches to the management of knowledge explained how the methods applied in one context can be transferred to the context of other functions with tangible benefits. In other words, this step allowed the researcher to understand why specific approaches are used (RQ2) and if they are transferred between functions. This concludes the case study protocol (CSP) in terms of its replication in each case.

Step 6: Leveraging IS Security

Step 6 utilises the cross-case analysis to identify themes emerging from across the two cases. There are various strategies to identify cross-case patterns, such as: selecting categories, searching for within case differences and similarities, the development of a matrix to compare several categories, and determine the differences. Additionally, it is through the adoption of a combination of these strategies that stronger theoretical insight is elicited. RQ3, by contrast, presents a cross-case analysis; a generic understanding of the relationship between IS Security and CS (or the KM environment) across the two case studies was built. The relationship between the functions at both a local level (within case analysis) and across the two cases was determined (Chapter seven). Additionally the different approaches to managing knowledge were synthesised to determine any comparisons and differences across the two case studies.

The collective purpose of RQ1, RQ2, and RQ3 was to understand the context of the CS and IS Security activities of the organisations and to determine how IS Security could leverage the concept of KM through qualitative research. Additionally, it was to highlight the issues which have emerged through the integration of the people (roles and responsibilities), the processes (classification of resources) and the technologies used. The findings from the lessons-learned within and across the cases theorise a possible approach to the management of IS Security knowledge. The research methods and protocol described enabled the researcher to achieve reliable and meaningful conclusions for this investigation and for the IS field in general.

3.6 Conclusion

The main contribution of this Chapter is to present and justify an interpretive approach as a means of inquiry for this investigation. The research methodology was selected due to the nature of the research topic and the various theoretical considerations. Research in information systems security has rarely been addressed methodically by using beliefs rooted in the interpretive paradigm. This Chapter stresses that theory building in IS Security can be accomplished through empirical investigation. The objective of this investigation is to interpret the complexities of a social phenomenon. Chapters five and six present findings of such investigations. However, to begin with, Chapter four presents the pilot study conducted to verify the data collection, analysis techniques, research lens and CSP used.

CHAPTER FOUR

TESTING THE CASE STUDY PROTOCOL

4.0 Introduction

The preceding Chapter discussed the research method selected to investigate the objective of this study. The purpose of this Chapter is to report on the pilot case study (Figure 1.1). The pilot case is used to allow the researcher to learn about the phenomenon before beginning work in the case studies selected for this investigation. Essentially the pilot case is used to test the data collection and analysis techniques, interview guide and the case study protocol. In the context of this pilot case study, the literature provided a lens (Figure 2.5) whereby the rich contextual description of the pilot case study was structured to present the findings systematically. The following section provides information on SERV-Co, the organisational infrastructure, the specialised units under analysis, their approaches to managing knowledge, and a comparison between the approaches used. Finally, the Chapter concludes with a summary of the findings and lessons-learned from this pilot case study.

4.1. SERV-Co: The Pilot Case Study

4.1.1 Organisational Background

SERV-Co (pseudonym) operates in three business divisions: (1) printing, (2) healthcare products and (3) supply-chain management. The company's printing division provides a comprehensive combination of printing and digital solutions to its consumers from digital content management to e-Business services. The corporation's global supply-chain management services division of operation provides outsourcing capabilities to some of the world's leading technology companies such as Dell. As explained by the GIS Manager "outsourcing has become very common in IT and other industries; it is regarded as intrinsic to their management". Services include: materials sourcing, product configuration and customised kitting, order fulfilment and global distribution. "Global companies want to improve their supply-chain due to the estimated eighty percent costs and industrial experts report that aggressive supply-chain management targets and achieves [a] thirty percent reduction in costs", as stated by the Project Leader. However, due to the complexity of end-to-end customer delivery, organisations utilise the competencies of companies such as SERV-Co to provide supply-chain integration. SERV-Co regards themselves as pioneers in supply-chain integration and offer capabilities amassed after twenty years of experience. Additionally its worldwide facilities provide consumers with a cohesive globally integrated service in three regions: (1) North America, (2) Europe and (3) Asia. SERV-Co is a global partner for leaders in the technology, medical, pharmaceutical and retail sectors. SERV-Co sells its services through the utilisation of its resource capabilities and information technology with those of complementary providers (such as logistics providers, technology service providers and business process managers) to give greater cross-functional capabilities and broader

autonomy across the supply chain from the planning to the distribution stage. “The planning process can be complex and SERV-Co analyses a company’s product flow to create a customised plan for vertical and horizontal supply-chain optimisation”, as explained by the Business Analyst. SERV-Co’s goal for the planning phase is to condense a corporation’s product entry points and therefore simplify its supply chain. SERV-Co operates in a business environment that is influenced by rapid technological advancement, high demand and short product lifecycles and therefore a high level of uncertainty. Threats such as viruses and regulatory constraints are considered significant. Challenges enforced by the company’s competitors – such as rapid growth, compliance and entry into new markets – has resulted in an organic growth of internal information systems and silos of individual and firm specific knowledge. This, coupled with IS Security challenges such as compliance and securing customer and internal systems, has put enormous pressure on the organisation’s Global Information Systems (GIS) function. Relatively new regulations are having unexpected effects on the organisation, such as heightened IS Security awareness, increased documentation and business process reengineering. As explained by the SDLC Coordinator, “[the] Sarbanes-and-Oxley [Act] is forcing the documentation of internal processes, the assignment of responsibilities and [the] segregation of duties to ensure that [financial] scandals such as Enron will be avoided in the future”. The Act is placing significant strain on multinationals in general, specifically on their resources and time. SERV-Co “is separating core systems [due to regulatory requirements] and attempting to utilise [a] KM [strategy] to become more efficient”, as explained by the Project Leader. “SERV-Co for the time being is focusing on the implementation of a knowledge management system [called] iViewXT”, as stated by the DB Administrator.

With respect to this investigation, Table 4.1 provides an overview of the data gathered from multiple sources within SERV-Co.

4.1.2 Organisational Infrastructure

The organisational infrastructure is the foundation on which KM resides and is composed of: organisation culture, structure, communities of practice (CoP), common knowledge and IT infrastructure (section 2.6.5). These components for SERV-Co are discussed in the next five sub-sections.

4.1.1.1 Organisational Culture

Organisational culture reflects the beliefs which guide the behaviour of SERV-Co's employees. As explained by the GIS Manager “the majority of employees in SERV-Co have spent their careers with the company and have [therefore] acquired an infinite amount of knowledge”, that pertains to SERV-Co. Currently the culture of the organisation and its functions operate from the fact that “the company has been one which supports long-term employment supporting informal networks of information and knowledge sharing”, as stated by the Business Analyst. The regulative nature of the environment and customer requirements, have forced a culture of compliance as opposed to security awareness and knowledge sharing. The [Cork] Security Officer would disagree as “management at senior level do not understand the importance of security, when [or] if it affects them [slows down PC processing speeds] they want it [virus scanning software] removed”. Additionally, “employees are not penalised for breaking security policies”, as stated by the Help Desk Manager. Non-adherence to

security policies and lack of managerial support severely impacts the strength of the security controls implemented in any organisation.

4.1.1.2 Organisational Structure

Organisational structure is complex in a multinational organisation. SERV-Co is based in the U.S. with "the international arm of the organisation in Cork, Ireland. A vice-president who heads up each function is responsible for developing and implementing functional policies across all [of] the manufacturing sites worldwide", as stated by the GIS Manager. Additionally, a General Manager who is supported by a management team manages each of the manufacturing sites. SERV-Co operates a centralised IT and IS Security function called Group Information Services (GIS). As stated by the ITIL Coordinator "GIS reports directly to the U.S. and there is a VP [Vice President] for Europe but his focus is primarily on JD Edwards [ERP System] and sourcing new customers". "The VP is becoming more and more interested in our ability to comply with whatever regulations our customers are forcing us to comply with", as stated by the Compliance Coordinator. As stated by the CS Manager, "the ultimate goal of SERV-Co is to deliver whatever the customer wants and we [CS] along with IS [are] determined to meet those needs".

4.1.1.3 Common Knowledge

Common knowledge helps integrate employee knowledge through the provision of a common language. SERV-Co "employees are supply chain experts and depending on the market we are targeting, like for example healthcare. We will become experts on healthcare and the names for surgical instruments or hard drives for storage companies will be embedded in our minds", as explained by the Business Analyst. According to the Senior QA Engineer, "SDLC is fixed onto everything we do now because of compliance. It is SERV-Co's answer to complying with rules and regulations regarding access to the information needed". The systems development life-cycle is "a methodology to help manage and assign resources to existing and new projects", as explained by the SDLC Coordinator. Procedures for assessing quality, and "specialised business information [procedures and workflows], after a while becomes pretty common but still valuable", as explained by the QA Engineer.

4.1.1.4 Physical Environment

Physical environment is an important consideration in supporting KM. As explained by the ERP Analyst "the [physical] layout of our offices isn't the greatest for collaborating with the other groups. It used to be open plan but a couple of years ago we were separated from GIS which is on the floor above us now and we are at the other side of the building". CS supports the different SERV-Co subsidiaries throughout Europe and "we travel to those sites, for a few weeks, to oversee the implementation of the ERP system to make sure everything meets our standards. [However], when we return usually something has changed and because things are fairly closed now it's difficult to get up to speed". As described by the GIS Manager, "the States [corporate headquarters] determine our goals and we have no choice but to target them, we do collaborate but only over the phone or by email".

OVERVIEW OF SERV-Co									
SERV-Co -Multinational, -Engineering - 22k Employees -€1.5 Billion	**Industry Sector**		**Customers**	**Products**		**Competitors**	**Partners/ Vendors**		
	Supply Chain Management – serves as a global outsourcing partner to technology and medical products companies.		HP, Dell, Sun Microsystems, Abbott Medical Devices	Sell an entire Supply Chain		Any Supply Chain Management Company	Dell		
	Corporate Strategy		**Mission**	**Subsidiaries**		**ISS Function**	**CS Function**		
	Outsourcing company of choice – sell expertise		To be the first SCM company of choice	Cork, Ireland,		Full function is displaced throughout the Org	Support different facilities as well as Customers		
Interviews	**IS Security Function**			**Customer Support Function**			**Other**		
	Role	**Years**	**Subsidiary**	**Role**	**Years**	**Subsidiary**	**Role**	**Years**	
	• GIS Manager • Security Officer /Analyst • Security Officer /Analyst • Infrastructure Manager • Security Officer 2 • Compliance Coordinator • Access Mgt/ITIL Coordinator • Help Desk Manager • DB Administrator	12 4 7 2 2 4 3 6 8	U.S. U.S. Cork U.S. U.S. U.S. Cork U.S. U.S.	• CS Manager • CS Engineer • ERP Analyst • Senior QA Engineer Quality Assurance • Project Leader • Business Analyst • SDLC Coordinator	9 12 5 4 6 8 2	Cork U.S. U.S. U.S. U.S. Cork Cork	• Director of HR • Manufacturing Trainer	10 4	
Documentation Analysed	**Security Documentation**			**Customer Support Documentation**			**Corporate / Public**		
	• SERV-Co Customised – ISO17799, ITIL & SecSDLC Guidelines • SDLC Template • Security Policies: Re: Segregation of Duties – by CFO, email, Internet, Remote Access, Corporate Policy • Business Continuity Procedures: Power Outage • Viewed: iViewXT ISS View • Viewed: Helpdesk Tracking System • Intranet: ISS Website			• Presentations: iViewXT Customer Presentation • iViewXT White Paper • Viewed: iViewXT CS View/ Customer View • Intranet: Customer Services (GIS) Website • JD Edwards (ERP) User Manual • SDLC GIS Documentation • SERV-Co Website – www.SERV-Co.com			• Annual Reports: • 2006/2007 • SERV-Co PR Pack / Organisation Chart		

Table 4.1: SERV-Co Data (Adapted from Tables: 3.3 (Roles & Responsibilities of the Interviewees) & 3.4 (Case Documentation Analysed)).

4.1.1.5 IT Infrastructure

IT infrastructure facilitates an organisation's KM infrastructure. As described by the Infrastructure Manager, "SERV-Co utilises enterprise resource planning. [ERP] enables the integration process that is used [by the company] to shorten customer supply chain to reduce inventories and costs". Throughout the planning phase SERV-Co will analyse customer processes and determine "how to apply IT, global management and tracking of product quality, inventory, distribution status and product life cycles", as stated by the Business Analyst. The sourcing phase increases a company's efficiencies by leveraging its purchasing volume and therefore reducing costs. "SERV-Co's IT infrastructure must allow us to integrate with our customers [for example] communication network and meet whatever requirements they have, which could be to connect with a VPN or provide them with an encrypted channel when accessing our support system iViewXT", as explained by the IT Infrastructure Manager.

This concludes the description of SERV-Co's organisational infrastructure as outlined in Step 1 of the Case Study protocol (CSP) discussed in section 3.5.

4.1.3 Customer Support Function

KM is a group specific initiative within Customer Support. Ultimately "SOX has brought unforeseen benefits such as [the incorporation of methodologies like the] SDLC to force the documentation of processes and lessons-learned", as stated by the SDLC Coordinator. SOX has also forced management and employees "to document every process and adhere to security procedures and standards as failure to do so could result in financial loss", as explained by the SDLC Coordinator. It is interesting to note that prior to the introduction of the SOX auditing process "very little was documented and lessons-learned from projects were not formally requested or required", as explained by the CS Manager. Methodologies were not utilised and duplication of information (as a central repository did not exist) was common. However, the allocation of resources and time taken in documenting everything, testing controls, formalising processes, essentially complying to auditing requirements has put an enormous strain on resources and some customer contracts have been lost or neglected as a result. "While SOX has had advantages, it is regarded as overkill and could be less demanding in terms of reporting demands", as stated by the [U.S] Security Officer. SOX has placed significant pressure on the CS and ISS functions in ensuring that employees have access/authorisation to the systems that they need to do their jobs. Compliance auditors request a significant amount of information regarding the segregation of duties within the organisation and it is the responsibility of both ISS and CS to ensure that this is achieved.

The following section identifies the different types of knowledge utilised by the CS function.

4.1.3.1 Types of Customer Support (CS) Knowledge

The different types of CS knowledge are described in the next three sub-sections. The first section describes the general knowledge necessary for the members to conduct their day-to-day operations. This knowledge is categorised as general as it is available to the CS function working throughout the organisation.

General knowledge common to the CS function is specific to supply chain management processes. As stated by the CS Manager, "documentation, procedures, guidelines are all stored on iViewXT so that everyone can access anything that they need". "Software and hardware specifications are stored, shared and accessed through the [iViewXT] repository", as stated by the Project Leader. As explained by the ERP Analyst, "guides for JD Edwards and SDLC are stored on iViewXT".

Technically specific knowledge is specific to the CS function. According to the CS Manager, "the SDLC is applied to all of the projects within SERV-Co to implement major projects, change requests and emergency changes to IT systems". The SDLC is a process of implementing enhancements or modifications, roles and responsibilities, steps in the process and deliverables from each step. As explained by the SDLC Coordinator "the model addresses changes to business systems, particularly the ERP system which includes modelling, configuration and testing". The SDLC is an evolving process and "will be continually updated as business needs change or process improvements are implemented. It is planned that every three months the Senior Quality Assurance Engineer will review the SDLC process and [the Quality Engineer will] update the document if required", as explained by the Business Analyst.

Contextually specific knowledge within the CS function of SERV-Co is used to solve customer problems. As stated by the CS Manager, "queries from customers are either phoned in or through iViewXT. They can login and contact us through the system". "Customers can access documentation or track the progress of their job", as stated by the Project Leader. "Reports regarding product configurations or trouble-shooting guides are available through what is essentially a self-service platform", as explained by the DB Administrator. Contextually specific knowledge pertains to the supply chain provided to a specific customer.

4.1.3.2 Reservoirs of Knowledge

Knowledge pertaining to the SERV-Co CS function resides in several different locations within the organisation. They encompass people and groups, including Engineers, Technicians, HR, management (CS and Engineering) and groups/teams (CS, Design and Product Engineers); artefacts, including procedures, repositories; and organisational entities, including organisational units, and inter-organisational networks. The reservoirs of knowledge are discussed in the rest of this section.

Customer Support as a function views the **people** working within the function as its greatest knowledge source. "Business Process Analysts are essentially internal ERP consultants. They are highly knowledgeable in the configuration of the ERP system, business models and best practices", as stated by the CS Manager. "The different [operational] sites worldwide maintain a small on-site IT staff including a Business Analyst and Technical Support technicians", as explained by the Manufacturing Trainer. As stated by the CS Manager, "Project Leaders are responsible for guiding a new project for a customer and selecting the appropriate resources".

Groups are created to support particular customers and their requirements. The following are the roles and responsibilities of a typical Customer Support team: the client is the consumer of the service provided by CS. The site Business Analysts are responsible for submitting a project request and gathering requirements from the client when the project is initiated at the site. As described by the CS Manager, "the Analysts gather all requirements from the client and document these in the business requirements

specification document stored in iViewXT, create a business process model, configure the ERP system and system test the application". Implementation support includes liaison with client and rollout, training, documentation, and handover of support to the Enterprise Service Centre. The nominated Project Leader is responsible for programmers, software development activities and deliverables of specific projects. "Project Leaders work closely with Analysts in delivering business solutions", as further explained by the CS Manager. The Group Programmer/Analysts are responsible for technical design, coding, as well as unit and integration testing.

Knowledge is **stored** in **artefacts** such as best practices, technologies and repositories. **Practices** can be organisational routines and procedures. "The SDLC is used as a template to document every process from the development of the different systems to an audit", as stated by the SDLC Coordinator. The documents are created from a template. The templates are used so that they can be stored and searched through iViewXT. A considerable amount of knowledge is stored in SERV-Co **technologies** and systems.

As explained by the DB Administrator, "the KMS [iViewXT] and the recent adoption of the systems development life cycle are attempts to formalise knowledge processes but it is just documentation and it is primarily based on the current project employees are working on. It does not explain to employees how solutions were obtained, who in the company is an expert in a particular field or the different customer models under development or in use. In fact there is no formal mentoring in place or an up-to-date skills database".

SERV-Co's customer base is significant and to facilitate its relationships with both customers and suppliers it required large volumes of information to ensure the operation of the different processes (depending on the requirements of the customer) run correctly. "Until the introduction of the company's web-based system (iView) all of this data/information was collected, transferred and archived through SERV-Co's ERP system with reports generated manually and distributed through email to its network of customers and suppliers and due to this manual approach the system was prone to errors and subject to considerable delays", as stated by the DB Administrator.

In order for clients to track their jobs or for suppliers to verify stocking levels, prior to the introduction of the web-based system, they had to wait until a report was distributed by a SERV-Co Analyst. This resulted in two main problems: (1) it took forty-eight hours to generate reports, which dramatically affected decision-making (2) and ad hoc reporting was not an option. Customers could not query the data to produce reports that were relevant to their individual needs. To alleviate these issues the company decided to develop a web-based integration tool to monitor products at any point in the supply chain as well as allow customers and suppliers alike to track their products/jobs. When the system was first implemented it was used by six organisations with twelve users using from seven to ten reports which increased to seven hundred users in seventy-five organisations using up to fifty reports. The primary drivers behind the adoption of a web-based integration tool were as follows:

- Shareability – utilising a web platform enabled the organisations with web-browsers to access the system and view their data in HTML.
- Low cost of entry – distributing the reports through the web dramatically cut costs in disseminating the information.

- Ease of implementation – utilising a web platform simplified the development and resulted in a more efficient method of communicating with both customers and suppliers.

SERV-Co's primary objective for the development project was to make information from its ERP system and other internal systems accessible to everyone in the supply chain. To do this, "the system was designed to provide [secure] ERP reports in real-time to give customers a complete view of the business processes to facilitate decision-making", as explained by the SDLC Coordinator. This therefore provided them with access to relevant information and generated ad hoc reports in real time to reduce both costs and cycle times.

Knowledge is also stored within **organisational entities**. As explained by the CS Manager, "the function operates closely with GIS and Finance. Access to our different systems and connections are determined by Finance and implemented by the Help Desk". The organisation does collaborate with partners and customers to form mutually beneficial **inter-relationships** through iViewXT "to allow customers to solve their problems themselves", as stated by the Senior QA Engineer. "SERV-Co has an established a network of global manufacturing and distribution facilities located in key markets of the Americas, EMEA and Asia Pacific. They execute critical elements of the supply chain including materials management, customised complex kitting, and fulfilment services", as explained by the CS Engineer. SERV-Co creates value by helping customers to increase their supply chain efficiencies and deliver products more cost-effectively on a global basis. SERV-Co applies information technologies throughout the supply chain to achieve process control thereby increasing capacity while reducing costs, cycle times and inventory requirements. The integration of SERV-Co's IT systems with those of their customers enables SERV-Co to become an integral part of its client's critical supply-chain functions.

4.1.3.3 KM Processes

This section describes the processes used to support the acquisition, capture, creation, sharing, application and control of knowledge in the SERV-Co CS function.

The **acquisition** of knowledge within CS function is not common. As described by the CS Manager, "information regarding a potential customer is sourced to prepare for a possible contract". "SDLC is an external method but it has been customised by CS to meet the function's and compliance requirements", as explained by the Project Leader.

Knowledge is **captured** or retrieved from the numerous knowledge stores. As stated by the SDLC Coordinator, "we use the SDLC [methodology] to pull knowledge from different employees or roles such as the different Analysts and force them to document every aspect of their job on a project". This process is enforced by a specific role in the CS function. "It is my job to make sure that everyone documents all of the different processes, workflows and even the access rights required for viewing the document or for JD Edwards [the ERP system]", as further explained by the SDLC Coordinator.

Knowledge is continuously **created** and **shared** through problem-solving. As described by the Project Leader "a new [customer] project is a new problem and we are allocated by our managers to solve the problem. The team uses iViewXT and SDLC to create the requirements documentation, and everything else we need so that we can all collaborate and solve the problem". As explained by the CS Manager "iViewXT allows us all to

share the documentation and answer questions so that we can save time and therefore money but also so that we are compliant".

Knowledge is **applied** throughout the different phases of the SDLC methodology. According to the SDLC Coordinator "the SDLC allows us to apply everything stored on one project to another. The lessons-learned are documented at the end of a project and they are supposed to be written up and then stored in the SDLC template and uploaded to iViewXT. If it isn't I have to track down the person responsible and make sure he enters the required information".

Knowledge **control** is necessary to assure the validity and utility of knowledge. According to the DB Administrator, "one of the key issues when developing the system was that of security. It was vital that the system was secure both from the external environment and between suppliers and customers". "In order to prevent user intrusions into segments they shouldn't access, SERV-Co introduced a ten character password to access the system", as stated by the CS Manager. Additionally, a firewall was positioned between the web server and SERV-Co's internal systems to reduce the risk of outside interference. "When a customer or supplier makes a request, it is routed through the web server to the application server where the request is processed. To generate the reports data is pulled from the iViewXT data warehouse", as explained by the DB Administrator. The data warehouse contains a sub-set of the enterprise applications database which is propagated with data from all of the internal systems to eliminate the need for a direct-link to the systems for both performance and security.

The system was developed using the J2EE and JSP open-source industry standards. XML was also included to allow users to export data. Microsoft SQL was used to construct the data warehouse. Finally, "data mirroring was used for replicating data, to achieve all of the requirements of the system, a technology that could pull data from a number of different internal systems [JD Edwards and the shop floor control and quality control systems] before exporting it to the iView data-warehouse", as further explained by the DB Administrator. The benefits that the system provided to the company are regarded as substantial as "it has strengthened our relationships with our customers and enabled them to have twenty-four support, access to information about their products and self-service, saving us time and therefore money", according to the CS Manager.

This concludes the description of Customer Support function operating within SERV-Co as outlined in Step 2 of the Case Study protocol (CSP) discussed in section 3.5.

4.1.4 IT/IS Security Function

GIS steers the IS direction, policies, security and technology standards used by SERV-Co. IS Security "is very much a part of the GIS group", as explained by the [Cork] Security Officer. As described by the GIS Manager, the function "is responsible for developing and implementing the IT strategy for managing major enterprise hardware and software and for implementing new customer solutions [in conjunction] with the IT personnel based at the [different] manufacturing sites". SERV-Co does not have a security group. A single security officer drives the different security activities affecting ISS. Therefore "information security is implemented through a community of practice operating within GIS with [specific] individuals assigned roles in assuring the protection of the organisation", as stated by the Compliance Officer. However, the structure of GIS is centralised and complex in nature; it consists of dedicated IS project managers who support the IT infrastructure of SERV-Co. The group is critical in

supporting new external projects and in supporting internal business units. The security analyst is responsible for security within the company and has a dual role as an internal auditor.

4.1.4.1 Types of IS Security Knowledge

This section identifies the types of knowledge utilised by the organisation's ISS group. The different types of ISS knowledge are discussed in the next three sub-sections. The first section describes the general knowledge necessary for the ISS function members to conduct their day-to-day operations. This knowledge is categorised as general as it is available to all of the IT professionals working throughout the organisation. Section 4.1.1 described the culture, structure and common knowledge used, all of which is regarded as general knowledge by the interviewees. Section 4.1.4 described the reporting structure of the ISS function itself which is fundamental to the group's knowledge of roles and responsibilities at a corporate and local level.

General knowledge common to the ISS functions is varied. "SERV-Co's current security model is driven largely by [the] ISO17799 standard, and risk analysis methodologies", as stated by the ITIL Coordinator. As explained by the Help Desk Manager, "SERV-Co uses operational and project risk combined with risk analysis methodologies, when assessing the level of security required by an application or system". The security policies utilised in GIS "are a corporate policy on IT risk and Security, business continuity policy, anti-virus policy, remote access policy and Internet usage policy", as stated by the GIS Manager. "[GIS] staff must know how to customise the different standards and best practices that we use so that they are effectively used and ultimately meet SOX", as explained by the Compliance Coordinator.

Technically specific knowledge is specific to the ISS function. External knowledge regarding environmental threats from vendors and online resources is vital. As stated by the ITIL Coordinator, "the group supports the security requirements of the different sites which are governed by Security Officers and [all of the] Security Officers collaborate". Ultimately new procedures are signed off by the VP and become company policy. According to the ITIL Coordinator, "new standards and frameworks are either recommended by the external auditor or we select something that will meet our needs". ITIL (Information Technology Infrastructure Library) is a customisable framework of best practices that promote quality computing. "The framework is under review and we have a few members of staff on training courses so that we get the best out of it and can prove to the VP that it will make audits easier", as stated by the Director of HR. "Audits are difficult and time consuming at the moment but they are getting easier with each one; we use SDLC to manage all of the documentation", as explained by the SDLC Coordinator.

Contextually specific knowledge within the GIS function of SERV-Co is primarily used to adhere to regulatory issues or for an incident such as a security breach. As described by the Compliance Coordinator, "knowledge about the different regulations that affect us and our customers is vital. [SERV-Co is] not a medical organisation but we still have to be compliant with HIPAA[12] as one of our customers operates in [the] health sector. SOX is an issue, a very expensive and time-consuming issue. SERV-Co has to adhere to SOX requirements and undergo regular audits". As explained by the

[12] The Health Insurance Portability and Accountability Act Of 1996, impacts all healthcare organisations. The risks for providers due to inadequate IS Security range from risks to patient care if records are doctored, liability of leaked information, loss of reputation and market share.

DB Administrator, “due to SOX we have to implement segregation of duties, access to systems has been completely redefined [as determined] by the Finance department”. “Security must identify everyone’s access [access control rights] requirements to the information or knowledge that they need to do their jobs”, as stated by the Help Desk Manager. “Security professionals must not only stay ahead of all the threats but also know how to comply with the different regulations and prepare for audits”, as stated by the GIS Manager.

4.1.4.2 Reservoirs of IS Security Knowledge

Knowledge, pertaining to the SERV-Co IT/ISS or GIS function, resides in several different locations within the organisation. They encompass people and groups, including IT and Security professionals, Engineers, management and groups/teams within IT/ISS; artefacts, including best practices, security technologies, and repositories; and organisational entities, including organisational units, organisations, and inter-organisational networks. The organisation reservoir is the SERV-Co organisation in its entirety. This reservoir of knowledge is described as part of the organisational infrastructure in section 4.1.1. The remaining reservoirs of knowledge are discussed in the rest of this section.

A considerable amount of knowledge resides in **people**. As explained by the GIS Manager, “the Security Officer or Analyst tracks employee access to the different systems. He is also responsible for implementing a change management process [utilised] to monitor changes to the different systems. Each subsidiary is allocated a Security Officer and they collaborate to share information regarding audits and different internal processes”.

The structure of the **groups**/teams working within the IT/ISS function is described in section 4.1.2. According to the Compliance Coordinator, “each [Security] Analyst is responsible for the regulatory requirements for their site”. A Group Internal Audit (GIA) “will act as corporate coordinators of the risk management process. GIA will, on a half-yearly basis, produce a consolidated Corporate Risk report for submission to the VP”, as stated by the ITIL Coordinator. “GIA, with the assistance of management will monitor and report on compliance with this policy to [the] external Auditor” as explained by the GIS Manager. According to Security Officer 2, “[GIA] will also review the continuing adequacy and completeness of policies and support reporting procedures and mechanisms used in SERV-Co”.

Knowledge is **stored** in **artefacts** such as practices, technologies and repositories. **Practices** can be organisational routines and procedures. According to the SDLC Coordinator, “information or knowledge pertaining to the different projects is stored, procedures are documented, and standards, emails / minutes regarding projects are typically stored in an access share”. “Project status information is stored in iViewXT and if the project requires the application of security standards and procedures such as customer applications it is listed and then allocated”, as stated by the DB Administrator. “General information is stored in iViewXT, typically emergency procedures are documented regarding the steps to follow in the event of a virus alert [which could result in loss of productivity]”, as stated by the [Cork] Security Officer. According to the SDLC Coordinator “mechanisms are in place to review and update security procedures so that security personnel can document lessons-learned from incidents”.

A considerable amount of knowledge is stored in SERV-Co **technologies** and systems. Information and knowledge are stored in one of the two main repositories by the members of GIS function. NT Shares are the main repositories used by the group with both aspects of the group (architecture and security) utilising separate shares. "Outlook is [also] used to store incoming documentation and messages. The Intranet is used as a repository for some documentation and iViewXT is becoming the central document repository", as stated by the ITIL Coordinator. Additionally, "monitoring tools are ineffective in providing an integrated view of the entire network", as stated by the [Cork] Security Officer. Therefore ISS technologies are not used to capture knowledge pertaining to corporate security network.

Knowledge is also stored within **organisational entities**. These range from the entire organisation, units within the organisation to **inter-organisational** relationships. The organisation as a whole is described in section 4.1.1. As explained by the [Cork] Security Officer "we collaborate with one another [other subsidiaries] and externally with the auditors; CS collaborates with SERV-Co customers through iViewXT".

4.1.4.3 IS Security KM Processes

This section describes the processes used to support the acquisition, capture, creation, sharing, application and control of knowledge in the IT/ISS function.

The **acquisition** of knowledge within IT/ISS is common. As stated by the [U.S.] Security Officer, "best practices, standards and frameworks like ITIL were researched, bought and customised". "The SDLC methodology was sourced externally and customised to act as a document management system (DMS) to ensure quality and responsibility as authors and Project Leaders are assigned to different stages of the methodology", as stated by the SDLC Coordinator.

Knowledge is **captured** or retrieved from the numerous reservoirs distributed throughout SERV-Co. As described by the [Cork] Security Officer, "collaboration is [primarily] by phone and we are implementing a change management process to make sure everyone participates in IS Security projects and for that communication between the site Officers and all of the SERV-Co employees is required". "Check lists from previous projects, [audit] reviews are pulled out and updated for the next project", as explained by the ITIL Coordinator. According to the [U.S] Security Officer, "we don't know yet which framework or standard is right but we are improving through the different security projects".

Knowledge is continuously **created** through the problem-solving process used within IT/ISS.

SOX have had a dramatic affect on the management of security knowledge as it is forcing the formalisation of policies and procedures. As stated by the [Cork] Security Officer "[the] auditing [process] for SOX is a learning process". The function is provided with feedback from the external auditor - Ernst and Young as a result of the audits conducted. "A significant amount of effort and processes have been put in place to reduce the amount of resources needed in auditing", as stated by the Compliance Coordinator. Additionally, the function utilises standards such as ISO17799 and ITIL for problem management.

The different Security Officers **share** knowledge during weekly meetings and actions are recorded in Excel spreadsheets. According to the [Cork] Security Officer "[the use of spreadsheets] is not viewed as very professional but it is regarded as an attempt to record project progression". Conference calls are "widely used to share knowledge across the organisation but the calls are not recorded", as stated by the [U.S] Security Officer. Action lists are uploaded to iViewXT for ratification by the global SERV-Co IS group. It is regarded as "very time consuming but the organisation needs to be compliant and SOX is a significant security activity", as explained by the [Cork] Security Officer.

The process of knowledge **application** or use is extensive in the IT/ISS function. As described by the GIS Manager "auditing has forced the application of knowledge gained from previous reviews. The lessons gained are reused for the next audit". Regulatory requirements have also forced the allocation of quality controls such as "security frameworks, and documents and project management methodologies like SDLC", as stated by the Help Desk Administrator.

Knowledge **control** is necessary to assure the validity and utility of knowledge. GIS aligns security measures (controls) to individual knowledge stocks. KM projects are implemented on an "ad hoc" basis resulting in the organic allocation of controls to numerous repositories which are not integrated. The size of the network and a false prioritisation of the assets have intensified the resources needed to "backup" and search through the individual and unit knowledge shares. The allocation of technical (access rights), formal (security policy) and informal (SETA) controls is creating sharing restrictions among and between the different business units. "The network is also audited to track communication to assure compliance with the SERV-Co security policy", as stated by the [U.S.] Security Officer. As explained by the GIS Manager, "SERV-Co employees have been affected by compliance as access rights to financial systems such as the corporate ERP system, [the] online web resources and internal knowledge or information repositories are controlled". "GIS group have applied security measures to implement segregation of duties", as explained by the Compliance Coordinator.

This concludes the description of IS Security function operating within SERV-Co as outlined in Step 3 of the Case Study Protocol (CSP) discussed in section 3.5.

4.1.5 Findings

SERV-Co has adopted a technological approach to its KM requirements. KM was not incorporated into the strategic planning of the company but as a core GIS and CS strategy to meet environmental drivers such as compliance and customer demand for support. Security measures, such as access controls, are applied to the "KMS". Access controls are used to partition the organisations systems and to enforce segregation of duties in accordance with the Sarbanes-and-Oxley Act of 2002. Fundamentally, it is the security activity compliance which has had profound implications on the management of knowledge within SERV-Co. It is forcing the organisation to develop, use and document processes. Prior to the enforced restructuring of internal processes and the partitioning of systems, the organisation did not utilise a secure methodology for the development of systems or document learning outcomes from customer related development projects.

The enforced utilisation of the SDLC methodology has resulted in the methodical documentation of project processes to increase learning and comply with regulatory requirements. However employees have stipulated that the level of documentation due to compliance has reduced the amount of time which they can allocate to knowledge sharing and even to projects. In fact projects have been lost or dramatically affected due to the amount of resources allocated to meeting regulations. Even though systems are audited the CS function is not privy to the review report as it is purely to adhere to environmental regulations. This report could ultimately track attempts to access the different knowledge reservoirs thus both protecting the security of the corporate knowledgebase but also allowing knowledge advocates to determine if the right users have access to the right knowledge. The adoption of standards such as ISO17799 and ITIL are forcing the organisation to apply a stepped approach to protect corporate tangible and intangible assets. Compliance to regulatory requirements has placed significant strain on the resources of GIS and particularly for security and Finance personnel. Compliance has had surprising benefits for the management of knowledge within the organisation. This is primarily due to the documentation and formalisation of processes in the GIS and CS functions. The utilisation of resources such as personnel and time have been considerable. The most significant KM activity within SERV-Co was the development and utilisation of the KMS – iViewXT. The development of which required the application of numerous ISS controls to limit access to users (segregation of duties).

The adoption of SDLC did define and identify roles and responsibilities for the different phases of the development process which forced the required documentation of lessons-learned and assured a level of quality in protecting the validity of the knowledge stored. However the researcher also identified an omission of a fundamental step in the development process when interviewing the KM advocates (the CS function). The users /employees were not consulted during the development of the system suggesting that the SDLC methodology was not employed prior to the commencement of SOX audits. Therefore the changes made, due to compliance, were purely environmentally driven and not used as an opportunity to gain a competitive advantage. Table 4.2 summarises and outlines the different ISS and CS activities identified in this pilot case study. The ISS activities are aligned with the identified implications for the CS function using a KM solution. Each ISS activity has an implication for KM. The impact of a KM strategy on the ISS function is also outlined. Finally the impact of management is provided. Governance directly impacts ISS and KM as it determines the resources allocated to the two functions and the political support necessary for success.

4.1.6 Conclusions and Lessons-learned

The use of the SERV-Co pilot case provided the researcher with useful insights into conducting case study research. In addition to the practical lessons-learned such as the effective use of a Dictaphone, transcribing and display matrices, the pilot case study allowed the researcher to fine tune the interview guide. The researcher used display matrices to illustrate examples of general, technical and contextual knowledge through a common setting such as a college. This proved successful in the two case studies investigated. Key informants were identified from the ISS and CS functions to review and verify the display matrices created.

The pilot case study illustrated the fact that KM was adopted purely as a silver bullet solution for selling the SERV-Co service to potential customers as interviewees used the words: data, information and knowledge interchangeably and the strategy was

predominately a technological implementation of a central repository (iViewXT). Additionally the pilot case study did not have a separate ISS function. ISS was structured as a part of IT or GIS. This contradicts the advice in academia and industry that the ISS function must be separate from IT in order for it to operate effectively.

ISS & KM Activities	**IS SECURITY ACTIVITIES**	**IMPLICATIONS FOR CS**
	Strategic planning lacks KM	Mismatch of KM strategy to IT
	SOX enforces segregation of duties	Access to reservoirs based on domain rights
	Access controls	Partitioning of knowledge
	Auditing of Systems carried out	Purely for SOX requirement and not used by CS
	Forced documentation of processes	Less time for sharing Knowledge
	Network controls (Firewalls, VPNs)	Dedicated connection/ Encryption of Knowledge
	Standards: ISO17799	Enforced control of access
	Systems Development Life Cycle (SDLC)	Step-by-step approach to documentation
	ITIL	Stepped approach to problem-solving
	SETA	Security aware employees
	General auditing	Reduces time for knowledge sharing
	System histories are stored	Useful if shared with KM developers
	Quality assurance	Time spent on reviews instead of sharing K
ISS & KM Activities	**CUSTOMER SUPPORT ACTIVITIES**	**IMPLICATIONS FOR IS SECURITY**
	SOX: processes are documented & assessed	Time and the allocation of significant resources
	Development of KMS	Allocation of ISS resources to secure the KMS
	SDLC – documentation	Application of controls & documentation
	KM Network controls	Time spent securing the connections
		Additional controls for dedicated connections
		Minimum exchanges of Knowledge between sites
ISS: KM Activities	**IS SECURITY KM ACTIVITIES**	**IMPLICATIONS FOR ISS FUNCTION**
	Lessons-learned are documented	Processes are improved
	No Security KMS	Filtering knowledge is difficult & time intensive
	Communities of Practice	Across function responsibility
	Conference calls, meetings	Site collaboration
	Action plans	Steeped approach to problem-solving
	Development methodologies	Security is considered during the IS development.
Managerial Impact	**IMPLICATIONS FOR MANAGEMENT**	
	Financial controller has IT governance role	Segregation of duties based on roles
	Full support for compliance	Allocation of resources
	Pushing standards	Incorporation of methods and new processes
	Certification	Increased skills
	No KM strategy	Ad hoc implementations of knowledge tools
	Limited budget	Insufficient monitoring systems

Table 4.2: The Interplay between the Functions.

Step four of the CSP allowed the researcher to test the CSP itself, the research lens and the interview guide in a practical setting. Even though the pilot did not meet the requirements (a separate ISS and CS function using a KM strategy) of this study the lessons-learned as a result helped to refine the research strategy. In the context of this study, the literature provided a lens for the investigation. The factors and outcomes identified in section 2.7.1 of the literature (Figure 2.5 and replicated in Table 4.3) acted as a basis for grounding the investigation of the approaches used to manage knowledge in two specialised functions. This equipped the researcher with a fitting framework based on prior research from which to initiate the investigation while allowing enough scope to enable additional factors, outcomes and implications to emerge from the contextual settings of the organisational environments participating in this study. The analysis of the data collected from the pilot case study did identify additional variables

(Table 4.4) which were incorporated into the research model for investigation in the two case studies described in Chapters five and six. Therefore this pilot case study established the validity of the different data collection, analysis and verification (key informants) techniques used by the researcher. Steps 1, 2, and 3 of the CSP were tested (Figure 3.1) to determine if they were of value in addressing research questions one and two. Additionally SERV-Co was used to allow the researcher to become familiar with the phenomenon.

VARIABLES	CODES	EXPLANATIONS
Types		
Explicit	Exp:	is codified, documented, archived and communicated
Tacit	Tac:	cognitive (beliefs, viewpoints and mental maps) and technical (know how)
Procedural	Pro:	is dynamic requiring skilled actions – knowing what
Declarative	Dec:	is factual information that is static and easily described – "knowing that"
Tech Spec	TSpec:	deep knowledge about a specific field through training and applied experience
General	Gen:	possessed by a large number and can be transferred easily
Reservoirs		
People	Pep:	individuals and functions CoP
Artefacts	Art:	repositories represents another method of storing knowledge
Procedures	Proc:	stored in practices, organisational rules, routines and procedures
Technologies	Tech:	stored in technologies and systems
Org Units	OrgU:	organisational units / Org / inter-organisational networks
Processes		
Acquisition	Acq:	process by which new knowledge is obtained
Capture	Cap:	process of retrieving knowledge that resides within people, artefacts /org entities
Creation	Cre:	Generating knowledge
Sharing	Shar:	explicit or tacit knowledge is transferred
Application	App:	the use of knowledge to guide decisions and actions
Control	Cnt:	protection of knowledge resources
Mechanisms		
Use	Mech:	organisational or structural methods used to promote KM
Technologies	Tech:	knowledge Tools
Infrastructure	Infra:	culture, structure, CoP, IT infrastructures, common k & physical environment
Impact		
People	ImP:	employee performance can be greatly impacted through KM
Functions	ImG:	functions performance can be greatly impacted through KM
Processes	ImPr:	to quickly adapt to changes in their environments
Org	IOrg:	improving corporate performance

Table 4.3: Operational Factors and Outcomes for this Study (derived from Figure 2.5).

Interplay	Inter:	cross over between functions	Emerged from the analysis
Control	Cnt:	informal / formal/ technical controls	
Access	Acc:	segregation of duties	
Compliance	Sox:	Regulatory impacts	

Table 4.4: Operational Factors and Outcomes for this Study (identified from the Pilot case study).

CHAPTER FIVE

EXPLORING THE CME-CO CASE STUDY

5.0 Introduction

In this Chapter the data gathered from the first case organisation is presented and discussed (Figure 1.1). As described in Chapter three, this study adopts an exploratory qualitative method and utilises a holistic case design approach consisting of two multinational case studies. This study uses a multiple method data gathering approach which triangulates the data gathered during the data collection phase of this investigation. The method consisted of a combination of semi-structured interviews with management, Customer Support Engineers, IT and IS Security technical experts in two specialised functions, and documentation in the form of corporate reports, archival material, newspaper reports, staff guidelines, security policies (regarding email, Internet, IP and non-disclosure agreements), ethical codes, and disciplinary codes, internal communications regarding IS Security, KM and email management notifications (Table 3.4).

The purpose of this Chapter is to address the first and the second research questions through steps 1, 2, 3 and 5 of the research protocol described and illustrated in Chapter three (section 3.5 and Figure 3.1) and tested in Chapter four. The analysis of the IS Security and Customer Support functions, within CME-Co, revealed that the approaches utilised in managing knowledge varies. By comparing and contrasting data gathered from these multiple sources, a more complete and balanced study was possible (section 2.7.1). Given the sensitive nature of the study with respect to the management of IS Security knowledge, the identification of key intangible assets, corporate environmental threats and particularly legislative requirements, the case organisation has been assigned a pseudonym, which is a condition of the researcher's authorisation to access the case and conduct and publish the study as it pertains to the organisation.

Boring (1963) stated that "the best fact is one that is set in context, that is, in relation to the other facts". The purpose of putting research into context is to add validity to the research and to situate it for the researcher (Miles & Huberman, 1994) and the reader. This Chapter consists of eight primary sections (5.1.1 to 5.1.8) to structure the case as required by the research lens (Figure 2.5 and described in section 2.7.1). Sections 5.1.1 and 5.1.2 describe the organisational background and infrastructure. Sections 5.1.3 and 5.1.4 describe the management of knowledge within the CS and ISS functions. Section 5.1.5 compares the approaches used by the two functions so that one function can learn from another. Sections 5.1.6 and 5.1.7 describe the mechanisms used to promote KM and the impacts at functional and organisational levels. Sections 5.1.7 and 5.1.8 conclude by highlighting the impact of compliance on the management of knowledge within the organisation (Table 5.12).

5.1 CME-Co

5.1.1 Organisational Background

CME-Co (pseudonym) is a technology company and a world leader in products, services, and solutions for information storage and management. The corporate mission is to help customers get the maximum value from their information. To achieve this objective CME-Co produces leading edge products and facilitates the integration of these products (hardware, software, services) into solutions which are delivered with or through partners. CME-Co has subsidiaries located throughout the world with its headquarters based in Hopkinton, MA and its main European manufacturing centre in Cork, Ireland. Table 5.1 provides an overview of the company's profile since it was formed in 1979.

PROFILE OF CME-Co	
1979	CME-Co began in 1979.
1986	CME-Co entered the computer industry in 1981 and in 1986 went public on the NASDAQ.
1988	In order to advance at an international level CME-Co opened a European facility in Cork, Ireland.
1990 's	The growth of the Internet in the 1990s rapidly increased the demand for information storage and as CME-Co had the right product to meet the demand of this expanding industry saw its revenue increasing to $385 million in 1992 and sustained growth through to 2000.
1993	In 1993 the company released its first software product, the SRDF, which enabled the company to expand its products in information storage and retrieval.
1995	The company overtook its primary competitor, IBM, as the mainframe storage market leader
1999	In 1999 Data General was purchased by CME-Co providing the organisation with an entry level product CLARiiON in the competitive mid-range storage market.
2000	CME-Co continued to grow rapidly and by the end of 2000 had reached $8 billion in annual revenue with a worldwide employee head count of 27,000. This accelerated period of growth also had an enormous impact on the CME-Co Cork facility as Cork continued to manufacture all of the CME-Co products and the following functions were added: international Finance, IT telecommunications, technical support, support centers, R&D and the executive briefing centre. By the end of 2000 there were 1,750 employees based in the Cork facility with 600 employees in non-manufacturing areas.
2001	The computer industry in general found 2001 to be difficult as it faced the first worldwide recession since 1975. CME-Co endured a 20 percent reduction in total revenue from the previous year with $700 million reported losses. However the company had built a strong balance sheet during the growth period with capital balances at $2.7 billion and assets worth $10 billion.
2002	In 2002, CME-Co acquired Prisa Networks for its storage area network (SAN) management VisualSAN product.
2003	CME-Co switched its diversification into software and services into high gear, begun under a new CEO in 2001, by first acquiring Legato Inc. for $1.3 billion in July, followed by its purchases of Documentum and VMware in October and December of 2003 respectively.
2005	The acquisition of Rainfinity in August 2005 added a storage virtualisation product targeting Global File Virtualisation. Through an acquisition of a Belgian software company called FilePool, CME-Co developed a data-archiving product called Centera. This content platform addressed archiving-specific needs of ILM in a rapidly changing technical environment.
2006	CME-Co bought RSA Security, Inc. and opened an R&D office in Shanghai, China.
2007	CME-Co announced that it would invest $160 million in Singapore to setup a new 15000 square feet development laboratory.
2008	CME-Co announced the purchase of Iomega Corporation.

Table 5.1: History of CME-Co (Corporate Documentation: Table 3.4).

In 1990 the company introduced the Symmetrix 4200 integrated cache disk array which enabled the company to compete as an independent storage provider in the storage market. Corporate development in the computer industry was extremely difficult in 2002 as the company saw a reduction or contraction in its growth. As described by the KM Champion, prior to the contraction in growth, "if there was problem money was thrown at it". Due to this decline, senior management had to identify resources within the company itself and utilise them more effectively. The company analysed internal processes as, in the case of dramatic growth, operations were, to a degree, sidelined to meet consumer demands and increase operational efficiency. With a recent series of acquisitions and partnerships, the company has grown and diversified its product offerings. It has over thirty-three thousand employees with a turnover of approximately twelve billion dollars (2007).

The organisation operates in a business environment that is influenced by rapid technological advancement, high demand and short product lifecycles and therefore a high level of uncertainty. Threats such as reverse-engineering, viruses and regulatory constraints are considered significant. The organisation treats competition as a means of learning and comparing its performance with its competitors. Knowledge management within the organisation incorporates developments in the external environment as a source of knowledge. According to the Knowledge Champion competition is constant, "even though we overtook IBM and took a huge market share from them we have continued to maintain an established customer base". Competitors also push the organisation to share more and more knowledge with their customers by making a "…wealth of knowledge available to them forcing us to do the same". This is explained further by the Compliance Officer, "you have to evolve with the market place and as our products become more impacted by additional technologies which are typically being enhanced with the use of security".

As described by the IT Manager, "companies are being, effectively bombarded by regulations so that if you are a U.S. multinational and you have got overseas subsidiaries you could be required to comply with local, State and Federal laws in the U.S. and you can then be impacted by broad EU regulations. This is complicated further by a hugely fragmented [security] market sector with over three hundred security companies supplying hundreds of different security products to comply with security requirements". So according to the [U.S.] Security Coordinator, "that type of fragmentation makes it very difficult for companies to understand that if they have different technologies from different vendors – are they compliant". The organisation has identified this issue as an opportunity to offer customers a full service in meeting their storage and regulatory needs. As a result the CME-Co product portfolio is wide and complex requiring significant expertise in supporting customer needs.

With respect to this investigation, Table 5.2 provides an overview of the data gathered from multiple sources within CME-Co.

OVERVIEW OF CME-Co									
CME-Co -Multinational, -Engineering -33k Employees -$13.2 Billion '07	**Industry Sector**		**Customers**		**Products**		**Competitors**	**Partners/ Vendors**	
	Storage and Technology Industry		Fortune 500 Companies		Symmetrix, Celerra, Centera, Network Attached Storage Servers and Clariion		IBM, HP	Dell, McAfee, Microsoft, Fujitsu Services	
	Corporate Strategy		**Mission**		**Subsidiaries**		**IS Security Function**	**CS Function**	
	The Customer always comes first.		"Guilty until proven innocent"		Worldwide – Cork Ireland, UK, EMEA and Australia		Displaced throughout Organisation	5000 Staff worldwide (Engineering in the U.S.)	
Interviews	**IS Security Function**				**Customer Support Function**			**Other**	
	Role	**Years**	**Subsidiary**		**Role**	**Years**	**Subsidiary**	**Role**	**Years**
	• IT Manager	8	Cork		• CS Customer Mgr	13	Cork	• Purchasing Mgr	13
	• Security Officer	4	Cork		• KMS Engineering Trainer	10	Cork	• Project Manager -Six Sigma	7
	• Remote Access Manager	10	Cork		• KDG Officer	2	Cork	• Operations Mgr.	11
	• Security Officer	5	Australia		• Engineering Trainer	4	U.S.	Exe Brief Centre	
	• Security Coordinator	10	U.S.		• KMS & DB Administrator	8	U.S.	• Learning Officer	6
	• Infrastructure Manager	11	Cork		• Technician Eng Level 1	2	Cork	• Former IT Manager	5
	• OISRM/Compliance Coordinator	2	U.S.		• Technician Eng Level 2	5	Cork		
	• Remote Access Coordinator	10	U.S.		• Knowledge Consultant	14	U.S.		
	• Corporate Security Officer (Compliance Expert)	7	U.S.		• Engineer Manager	13	U.S.		
	• GIS Director – by email	12	U.S.		• E-Services	8	Cork		
Documentation Analysed	**Security Documentation**				**Customer Support Documentation**			**Corporate/Public**	
	• CME-Co Customised – ISO17799 Documentation • Security Policies Re: email/ Internet/ Remote Access • Data Centre - Disaster Recovery Procedures • Business Continuity Procedures • ILM Guidelines and White Papers • Business Continuity Planning Paper • Intranet: OISRM Website/IS Department Website • CME-Co Website – www.CME-Co.com				• Primus White Paper • ILM White Paper • Power-Link White Paper • Knowledge link White Paper • KCS Double loop process White Paper • Views: Primus CS View/Power-Link - Customer • Presentations: Global Primus Status - 2008 • Intranet: Customer Services Website			• Annual Reports: 2001/2005/2006/2007 • Profits Soar by 20% on Storage Demand • Channel CME-Co • Presentations: CME-Co Review 2007 Compliant ILM Strategy	

Table 5.2: CME-Co Data (Adapted from Tables: 3.3 (Roles and Responsibilities of the Interviewees) & 3.4 (Case Documentation Analysed)).

5.1.2 Organisational Infrastructure Supporting KM

The organisational infrastructure is the foundation on which KM resides and is composed of: organisation culture, structure, communities of practice (CoP), physical environment common knowledge and IT infrastructure. These CME-Co components are discussed in the next five sub-sections.

5.1.2.1 Organisational Culture

Organisational culture reflects the norms and beliefs which guide the behaviour of CME-Co's employees. It is an important enabler of KM. As described by the Knowledge Consultant the organisation is: "trying to change [employee] mindsets because culturally knowledge is power and that's something that we are trying to change; changing mindsets is one of the hardest things ever". The Purchasing Manager added that, "mentoring is part of the corporate wide culture in enhancing knowledge sharing. Employees who have been perceived as gurus – mentor". Historically the culture of the organisation is very much founded on legend and some very dynamic Engineers have achieved the status of legends and even heroes. The company is rich in legendary tales of business daring and a culture of doing - whatever it takes to create customers for life. Many interviewees have explained two widely accepted CME-Co values which capture the essence of this customer driven organisation: guilty until proven innocent – "CME-Co will take responsibility for any customer issue irrespective of it being a [competitor] hardware or software problem", as stated by the Operations Manager. Additionally minutes equals millions - this concept underlines the fact that CME-Co understands that as their products are mission critical systems and any down-time could cost a customer millions of dollars. CME-Co as an organisation takes huge pride in its successes publishing them in the corporate newsletter. Pride in the organisation is intense and the entire organisation including its business units/subsidiaries share a very competitive ethos. According to a Level 2 Technician, "there's a culture here of getting things done and if you can cut to the person that's responsible for something and if that's the quickest way to get something done, especially in a crisis, that's how you do it". However, in the opinion of the CS Manager, "knowledge sharing is very much grouped specific, CS as a group has a knowledge sharing culture".

The business environment, and therefore customer requirements, has forced a culture of security awareness. According to the Corporate Security Officer, "changes in the regulatory environment and customer security enhancement requirements – storage [market] is now changing in terms of a culture of awareness...as opposed to a security culture". At a senior level, management are committed to enhancing security both internally and externally "to be an inherent part of every department's considerations", as written on the CME-Co website. As described by the IT Manager, "[the organisation] has a proactive stance on security". Traditionally, according to the Corporate Security Officer, "even for a storage company, pre 9/11, security wasn't on people's radar as much. Most of the change in security considerations such as product design, IS Security and all the rest of it internally began to increase afterwards". The IT Manager stated that, "some functions are better than others, generally speaking there is a very high sense of security and people will be mindful of things that we can't afford to have go-wrong, that could take our system out of service for hours or days". The challenge of establishing good management practices in a geographical dispersed environment is

difficult. It is "the [geographically] spread of the organisation which is an obstacle to a culture of sharing and control" which is cited by many interviewees. To explain the situation the Purchasing Manager stated that it is "a kind of learning experience for all of us to actually come to terms with dealing with different cultures and understanding ...it's fine when you are speaking face-to-face but it's a bit more difficult when you are dealing with someone working in our, for example, Chinese subsidiary over the phone".

5.1.2.2 Organisational Structure

Structure is complex in a multinational organisation. The reporting structure can impact the management of ISS knowledge. The Knowledge Development Group (KDG) Officer stated that "the problem with such a big organisation [is that] different groups go away and do their own thing". The Knowledge Champion explained it further by stating that, "…all these different geographies are making it [KM] far too complex". As described by the Knowledge Consultant, "CME-Co is a company that has grown from small to big very quickly; to a certain degree…knowledge is being managed like a small company where the Engineering group would not be willing to open up content to us [CS]. A lot of it is historic, in how the company grew - we've always had access to this and never that so they would want to know why would we want it all of a sudden". The CS Manager explained that for commercial reasons, "internally there are separate organisations - it's two-pronged really". Essentially, in the opinion of the CS Manager, "Customer Support sits in between [Engineering and the customers] and there is a reluctance to release information to us in case it leaks out to sales or to the customer base and we keep telling them - look you can trust us, but they are still reluctant".

The company did undergo a reorganisation to centralise the different point-of-contacts for customers. As described by the Knowledge Champion "the organisation went through a reshuffle, a year or two ago; it used be managed in each GEO by different directors so the reporting mechanisms were different. Now you've got one director overseeing certain products globally so the infrastructure is there to allow the knowledge infrastructure to be built up in the same type of hierarchy". This is necessary, as the Knowledge Champion further explained that, "there's no point in us having you know one set [of reporting layers] over here and whatever they use in Asia - it needs to be consistent globally". Basically, according to the CS Engineer, "the calls rotate to wherever the sun is shining so if it's bright over here we have to know if you are dealing with the same customer; you need to be referring to the same content, the same console, so you're giving him the same information, and not one guy saying one thing and another guy saying another thing because they are looking at different files".

As described by the IT Manager, "CME-Co is a very centralised company with its headquarters in the U.S. so while we [IT] support the business functions a lot of our core systems are actually physically located in the U.S. and our users are remote users of those systems, so that tends to make it quite complex if you're looking for specific information as the answer to that or the knowledge is [located] in the U.S. or sometimes it can be here [in Cork]". IS within CME-Co Ireland facilitates or supports every business unit operating in Europe reporting to the Global IS (GIS) Director in corporate CME-Co. According to the [Cork] Security Officer, "we [CME-Co] are fairly autonomous - if there is a corporate directive on something it will come from Boston". The last significant change was to move the Help desk function to the U.S. As described by the Remote Access Coordinator, "Cork was not happy at the time, a lot of autonomy

and control was lost". A new security group, OISRM (Office of Information Systems and Risk Management), was also established and based in corporate headquarters to source regulatory guidelines and best practices. Communities of practice are also used within the organisation. They are formed, according to the IT Manager, "when any project begins". These could incorporate the organisations external stakeholders such as customers and partners.

5.1.2.3 Common Knowledge

Common knowledge helps integrate employee knowledge through the provision of a common vocabulary. CME-Co's product portfolio is wide and complex requiring significant expertise in supporting customer needs. Product design specifications are considered common knowledge. According to the Level 1 and 2 technicians, "G.A [General availability] product specifications are regarded as common knowledge". Engineering terms pertaining to the status of a product and project management terminologies such as Six Sigma and M-Gates are examples of everyday vocabulary. As described by the Knowledge Consultant, "Channel CME-Co is our Intranet or our central point for all employees and that's where our CEO would have messages; it's a link to all of the websites in the company and it has general information on corporate procedures and methodologies". An enterprise-wide KM initiative in the form of a content management system has also, according to the CS Manager, "been launched – it's more of a common document repository though". He explained that it [the repository] stores "product information that we all need to do our jobs, such as SRDF[13] documentation". The Knowledge Consultant added that, "it's something people have been screaming for, for a long time…where we can join all of these disparate databases together into an overarching content management system".

5.1.2.4 Physical Environment

The physical environment is an important consideration in fostering KM. As explained by the KDG Officer "there's nothing better than [open plan] and getting up off your chair and going over to another person for help in solving a problem". Dispersed geographies or subsidiaries are difficult obstacles to solving problems. As described by the Knowledge Champion "tech support is located in one building [in Cork] and physically they are far apart from the Engineering group [in the States]. In the escalation process [for problem-solving] if a technician based in the U.S. Support Centre cannot solve a problem "you've got the Design Engineers [next door] and initially they'll phone the Engineers at the desk; if they still have a problem the Engineer will pop in the door and he's there and they'll sit down next to you [the technician]" as added by the Knowledge Champion. Unfortunately according to the CS Engineering Trainer "if we want to get the Engineer [in Cork] we have to get them by phone and they will ask us to disconnect from the Symmetrix [in for example a German bank] so that the Engineer can dial-in and have look at it, spend twenty minutes in there and then he'll come back and say "right it's fixed". However according to the CS Trainer, "the technician hasn't seen the process used to diagnose the problem [and it is also] rare enough that the Engineer would tell us to build a solution". The only solution, as described by the CS Manager, "is to physically rotate [Cork] Technicians enabling them to shadow Design

[13] SRDF (Symmetrix Remote Data Facility) is a family of CME-Co products that facilitates data replication from one Symmetrix storage array to another through a Storage Area Network (SAN) or IP network.

Engineers in the States and build relationships with them through face-to-face interaction".

5.1.2.5 IT Infrastructure

IT infrastructure facilitates an organisation's KM infrastructure. As explained by the IT Infrastructure Manager CME-Co uses, "a lot of communication technologies and access controls as logical types of security capabilities; you have also IP [Internet Protocol] based protocols in storage to provide greater data aggregation - in terms of company consolidating multiple data centres into fewer data centres". The Infrastructure Manager further explained that this type of infrastructure "leaves you with more eggs in one basket type of scenario to adhere to compliance type impacts to protect the data itself, not actually the networks, and the physical infrastructure of the company, so the focus has switched more from technology and security technology to the needs to secure the data itself". The Compliancy Coordinator stated that, "ISS is very firmly focused on preventing an issue happening and keeping threats out of the company". According to the IT Manager, "most projects would end up at some point having to be reviewed by security to make sure they are comfortable with the infrastructure that is being developed, that it is compatible with their security strategy, which should be aligned to the business strategy.

The organisational infrastructure characteristics are summarised in Table 5.3.

OVERVIEW OF CME-Co ORGANISATIONAL KNOWLEDGE	
DIMENSIONS	**CHARACTERISTICS**
Org. Culture	• Knowledge sharing is group specific Interrelationships depend on knowledge trading • The value of KM is recognised by management but controlled by Engineering • An awareness of Security • Knowledge creation is encouraged at a group level but not across the organisation • Competition internally and externally is encouraged • Emphasis on leadership – for example hero status through stories • Multinational organisation with varied cultures and languages
Org. Structure	• Hierarchical structure with complete autonomy in the U.S • Communities of practice (CoP) are created for specific projects • Specialised units and roles are used – for example the creation of OISRM and the knowledge development group (KDG) • Corporate Security Officer, Compliance Officer & Knowledge Champion
Common Knowledge	• Common Engineering and Industry (Storage and IT) terminology • Shared values and norms • Recognition of domain specific knowledge – for e.g. IS Security or CS • Specialised knowledge, such as product specifications, available to CME-Co
Physical Environment	• Open plan office in each subsidiary • Geographic separation between International CS and Design Engineers • No specifically designed rooms for sharing (ISS/CS) knowledge • Face-to-face contact is very rare and rotations are considered vital
IT Infrastructure	• ICT is used extensively | Data aggregation & Consolidation of Data Centres • Security is aligned to the business

Table 5.3: Organisational Infrastructure Characteristics.

The next section describes the IS Security function's approach to managing knowledge.

5.1.3 Customer Support Function

CME-Co directly "services all of its product offerings", as stated by the CS Manager, making the multinational extremely customer driven. As explained by the Engineering Manager the organisation, "will do anything to create a customer for life". A global support operation is utilised to support the products sold by the organisation, "one of the primary products we sell is called Symmetrix which is a storage product. The support of the product is based out of three locations [Cork, U.S. and Sydney], and [facilitated] through the technical support arm or organisation [which consists of] three hundred and eighty members", as described by the CS Manager. The Customer Support (CS) function consists of support Engineers, Field Engineers and Trainers with Developers based in Corporate CME-Co operating as the highest level of support. As explained by the Knowledge Consultant, "Customer Support ensures the availability and integrity of data stored on CME-Co products in thousands of customer sites around the world. It supports customer upgrades, modifications and maintenance". CS is one of the key strategic units within CME-Co which, as described by the CS Manager, "operates like a silo organisation servicing customers throughout EMEA". The Knowledge Consultant explained that, "the company offers [or provides] its customers with entire mission-critical infrastructures – not just storage". "CME-Co monitors its customers equipment through the web using an unmatched remote support tool", as stated by the E-Services Manager.

As explained by the Engineering Manager, "the Symmetrix product has a call home feature that activates upon detection of a problem. Product support Engineers are then able to remotely diagnose the error codes and make the necessary adjustments, or dispatch a Field Customer Engineer for an on-site resolution". "When our systems phone home, the CS Engineers and Developers diagnose the problem remotely and work with customer Engineers in the field to resolve the situation", as explained by the KMS Engineering Trainer. CS also interfaces with "Research and Development, Engineering and the Executive Briefing Centre on product feedback to ultimately maintain the best customer service satisfaction in the industry", as stated by the Operations (Briefing Centre) Manager. However the Engineering Manager stated that, "control [in terms of interaction] between the different groups can vary depending on the product or more accurately its status. It doesn't matter if a manager in CS or in Sales requests a design or fix – if it's not G.A [general availability] no one gets access". This can prove difficult for a function like CS which is supporting a product "especially if a bug [problem] is known in Engineering and they have the fix – we could spend half a day or more trying to fix a fixed bug". Thus, existing solutions can and are restricted due to the risks identified or perceived by Engineering.

Customer Support, to become more productive, "identified KM as a strategy which could increase productivity and increase both employee and customer knowledge regarding CME-Co's product portfolio", as stated by the KMS Engineering Trainer. The function has pioneered the implementation of a KMS "to store solutions for the different experts working within CS", as stated by the KDG Officer. However the KMS Engineering Trainer, regarded by the majority of those interviewed as the organisations Knowledge Champion stated that, "Primus is just a technological solution to the KM problem within CS". The CS Manager also explained that the current, "corporate KM initiative is just a content management system and [essentially] just a Marketing public relations KM initiative". "We [CS] don't even think of it as knowledge management to

be honest", as explained by the Engineering Manager. Global CS established a team to promote knowledge management for supporting customers. The KCS (Knowledge-Centred Support) team was created "to help implement knowledge management within CS. The team was not set up with experienced knowledge management personnel but with people from the existing CS Engineering group with some technical training behind them", as stated by the KMS Engineering Trainer. As a result, the members of the function were according to the Knowledge Consultant "experienced CS Engineers who had an interest in knowledge with little formal training in regards to the whole KM concept". "The KCS team are responsible for knowledge management in the CS function and they advocate the use of knowledge management and the Primus system", as explained by the CS Manager. Team members are primarily "trainers and technical writers assigned from each site to ensure that Primus is used to carry out the necessary activities for [the] creation, storage, and reuse of knowledge", as stated by the KDG Officer. "The Primus system is co-ordinated by the KCS team – they approve all solutions before they are submitted to the Primus database" as further explained by the CS Manager. The Knowledge Development Group, was created to work with CS and the KCS team "to develop skill sets throughout the organisation", as explained by the KDG Officer. Each subsidiary has a KDG Officer "to identify, coordinate and run training for CS using [platforms like] Knowledge-Link and specialised training courses", as stated by the KDG Officer.

The following section identifies the different types of knowledge utilised by the CS function.

5.1.3.1 Types of Customer Support Knowledge

The different types of CS knowledge are described in the next three sub-sections. The first section describes the general knowledge necessary for the members to conduct their day-to-day operations. This knowledge is categorised as general as it is available to CS function practitioners operating throughout the organisation.

General knowledge common to the CS function is specific to the product portfolio. As explained by the Level 1 Technician, "you can find just about everything you need about the company on Channel CME-Co [the Intranet]. If I need to lookup documentation on regulations, policies or someone in GIS or a department head I can do a search". However, as explained by the Level 2 Technician, "it does take time to build up a contact list for the different systems or products". "Hot issues of the day [regarding coding errors] are important so people are encouraged when they login to look at email notices [internal and vendor specific]", as stated by the KMS Engineering Trainer. He further explained that, "there could be a warning about drive errors, from Engineering, and a link to training materials, technical procedures for different aspects of the product and descriptions of errors, so a warning [email] could contain a wealth of information and could save a Techie time". "Design specifications for the box [Symmetrix] and other products like our drives are fairly well known especially if you have been working here more than six months", as stated by the Level 1 Technician. However the portfolio "is wide and complex requiring significant expertise in supporting customer needs", as stated by the KDG Officer.

The next sub-section describes the technical knowledge utilised by members of the CS function.

Technically specific knowledge is specific to the CS function. User guides for the numerous products are vital but according to the KMS Engineering Trainer, "there's no point in having the same content as the customer so when the customer rings, you need to have a much deeper level of knowledge of the product, you need to have operational knowledge – how is this thing designed, architected, constructed, coded all the way up". Documentation such as "White Papers, downloaded from vendor [HP] sites are used and customised", as stated by the Level 2 Technician. These sources "help with minor problems but deeper skill-sets are needed to support the kind of knowledge that is required for some bugs [such as] the inner workings of the product", as stated by the KMS Engineering Trainer. As explained by the Engineering Manager, "it's not just explicit knowledge; there's a lot of tacit knowledge here [in diagnosing and fixing a coding bug] it's certainly not just the people, it's delivering mechanisms like [Engineering] seminars, training, performance [measures] training, websites, the ability to find [existing and create new] solutions, presentations and [email] warnings, it's a whole load of different mechanisms and tools". Customers can also access technically specific knowledge through Power-Link, the organisation's Extranet. As described by the KMS Engineering Trainer, "customers can access the CS knowledgebase through their own support page [Power-Link view], they can limit their search or query for a particular product or problem as we have about twenty-thousand solutions available to customers". Customer solutions are explicit in nature "they never contain advice or opinions such as lessons-learned from previous, for example, solutions. These are similar to troubleshooting guides to ultimately save CS time [and money] and provide a pool of experts as a service to our customers", as stated by the CS Manager.

The next sub-section describes the knowledge used for a particular circumstance or problem.

Contextually specific knowledge within the CS function of CME-Co is primarily used to solve customer problems [calls or fixes]. Technicians and support Engineers need to be able to "effectively trace the problem through the product's development so a lot of the time we simply reverse-engineer it – especially if some [code or bugs] are not available", as stated by the KMS Engineering Trainer. The CS Manager further explained that "it's not how to use [the product] it's not what it does [as described in manuals and White Papers], it's how everything is connected, what happens when this goes wrong and that goes wrong, it's essentially the what ifs and how's". As explained by the Engineering Trainer, "CS's experience at handling hundreds of similar symptoms, combined with the customer Engineer's expertise and knowledge of their customer's particular operating environment help solve the many problems that come through the CS function on a daily basis. They also rely on a knowledgebase that allows customers access to solutions that have been created". Therefore CS contextually specific knowledge is focussed on interoperability problems.

Table 5.4 summarises the different types of CS knowledge identified within the organisation.

CUSTOMER SUPPORT FUNCTIONS: SUPPORT KNOWLEDGE						
Types	**General Knowledge**	**Role**	**Technically Specific**	**Role**	**Contextually Specific**	**Role**
Declarative						
Explicit	Documentation describing: CME-Co, Stock options	O	A document describing: CS & Engineering Regulations	O	A (solution) template outlining the requirements of a solution for reuse	O
	Organisational Chart & list of contacts for critical systems	O	A document describing: how a product works	O	List of known errors & bugs for the Symmetrix	O
	CME-Co Product specifications	O	A document describing: how a Vendors product works	O	List of solutions for training CS members in supporting the Symmetrix	T
	List of emailed daily warnings & links to solutions	O	A document describing: a Customer's Environment - interoperability issues	O	CS Training manuals on procedures & specific products	O
	List of Errors: regarding product/s	O	Products bugs or new errors – issued by Engineers or Vendors	O	List of Vendor bugs for Symmetrix interoperability	O
Tacit	Knowledge of the Regulations pertaining to CME-Co	O	Knowledge of the factors to consider in implementing Regulatory Requirements	O	Technician's knowledge of Symmetrix Errors	O
	Knowledge of the priority of Hot Issues	T	Knowledge of the factors to consider when diagnosing an error	O	Engineer's knowledge of different risks associated with the Symmetrix	O
	Knowledge of the different levels of support	O	Knowledge of interoperability problems with Vendor products.	T	Engineer's knowledge of lessons-learned in coding the Symmetrix for others to use	O
	Knowledge of CME-Co Roles & responsibilities	O	Knowledge of the potential bugs & impact.	T	Knowledge of diagnosing Symmetrix bugs	O
	Knowledge of external experts	O	Engineers knowledge of sources of solutions	O	Knowledge & impact of Vendor bugs	O
Procedural						
Explicit	Emails describing bugs for different products & the solution steps	O	List of Errors & Solutions to Product bugs	O	Solution with sequence of steps a Technician should take in the event of a coding error	O
	Emails describing Vendor specific errors & steps	O	A manual /KMS artefact describing a Solution	O	Feedback from customers regarding solutions or response times	T
Tacit	Knowledge of the steps to align a solution to an error	T	CS knowledge in Diagnosing a Solution	T	Knowledge of steps to take in diagnosing a Symmetrix error	O
	Basic knowledge of the steps needed to find or create a solution	O	CS knowledge of the steps necessary to solve a problem	T	Knowledge of the steps to take to reverse-engineer the Symmetrix & Vendor products	T
* Knowledge Roles: Operational = O; Tactical = T and Strategic = S						

Table 5.4: Types of Customer Support Knowledge.

5.1.3.2 Reservoirs of Knowledge

Knowledge, pertaining to the CME-Co CS function, resides in several different locations within the organisation. They encompass people and functions, including, Engineers, Technicians, Trainers, Knowledge Consultants, Management (CS, Engineering and E-Services) and groups/teams (KCS and KDG) within Customer Support. Artefacts, including best practices, security technologies, and repositories are used. Organisational entities, including organisational units, organisations, and inter-organisational networks are also sources of knowledge. The organisation itself, in its entirety, is a knowledge reservoir. The reservoirs of knowledge are discussed in the remainder of this section.

Customer Support regards **people** within the function as its greatest knowledge resource or asset. As explained by the CS Manager, "the main knowledge asset we have is definitely people, without a question". "We do rely very heavily on the systems like Primus but if our system [product] experts walked away [Primus] wouldn't really be hugely helpful to us, without the experience of the people", as stated by the KMS Engineering Trainer. The KDG Officer further explained that, "people feel that they can learn more from their peers than from Primus". As described by the CS Manager, "[in problem-solving] it's what you know and who to call to find out where the solution [or part of it] is [stored]". "Typically if someone wants to be the go-to person for a particular skill or particular product it gives the expert a type of status", as stated by the KMS Engineering Trainer. However, according to the Knowledge Consultant, "Technicians or Engineers may not want to share [particular] knowledge that can affect their status as a Clariion guru, for example. Some people simply don't want to share information or knowledge for their own personal reasons".

As described by the Engineering Manager, "Customer Support and Engineering are structurally aligned along expertise or skills-sets". **Groups** are created to support particular products. Skills locators or matrices exist in CME-Co but, according to the Knowledge Consultant, "people just seem to know how to get the right person without having to use it [the locator]". An escalation process is utilised in ensuring the quality of the solutions created, stored and reused. As explained by the KMS Administrator, "a second pair of eyes is required to approve any solution – typically one of the KCS writers is used. It would be the subject matter expert in a particular support team that would be called on to review the solutions for the approval process". "The KCS team is relatively new [established in 2006] but the goal is to use the group to support the entire CS organisation", as stated by the Knowledge Consultant.

Knowledge is **stored** in **artefacts** such as practices, technologies and repositories. **Practices** can be organisational routines and procedures. "The CS uses a template for the creation of solutions so that they are correctly tagged [for CBR searches] and can be reused", as stated by the KMS Engineering Trainer. "This combined with the [call] escalation procedure allows us [CS and Engineering] to use our tacit [pool of experts] and explicit [stored solutions] knowledge", as stated by the Knowledge Consultant. A considerable amount of knowledge is stored in CME-Co **technologies** and systems. As explained by the Knowledge Consultant, "the KMS contains over thirty-three thousand knowledge articles [solutions] detailing best practices and problem solutions".

There are a number of **KM technologies** in use within CME-Co. As described by the CS Manager "Primus is the key debugging KMS and contains a repository of knowledge objects detailing best practices and solutions". Currently "Primus does not

link into Knowledge-Link [the online training portal]; although it is possible to attach a learning activity [from Knowledge-Link] to a Primus knowledge object [to enhance training]" as stated by the KMS Administrator. In fact, "the only reference to Primus made within Knowledge-Link is to an online course on how to use Primus", as explained by the KMS Engineering Trainer. There are numerous KM technologies used within CME-Co including a "managers" discussion forum which is available to managers as an Intranet application and a system called Engineer Alerts which is used by employees within manufacturing for problem management", as stated by the Engineering Manager.

Knowledge is also stored within **organisational entities**. The units are structured for "commercial reasons with CS sitting in between Engineering, which are effectively the R&D folks who design the product and manufacturing, and customers", as stated by the CS Manager. The CS also interfaces "with other groups such as IT, ISS, Engineering, PPMG and the Executive Briefing Centre regarding product feedback and IT services", as stated by the Operations Manager, to ultimately maintain its customer-base. "IT and Security are consulted through PPMG when we need to change access rights to any of our systems or work with an external company or customer", as stated by the KMS Engineering Trainer. As described by the Knowledge Consultant, "security [the function] are used to keep us out of the Engineering systems or to enforce segregation of duties". The objective or goal of adopting a KM approach in CS is "to push knowledge toward the customer as the longer it takes for a customer's problem to be solved [from the time the call was logged], the more layers of support it is escalated through, increasing cost and the utilisation of [Engineering] resources", as stated by the Engineering Manager.

As explained by the CS Manager, "group interaction or sharing with the Engineering organisation can be problematic. They are scared stiff one of the product designs getting out to the customer base [through for example Power-Link] or to the Sales organisation". Additionally, "if Sales get any kind of sniff that there are serious deficiencies within the product, for instance, then they won't sell it", as further explained by the Operations Manager. The KMS Engineering Trainer explained that "[a few years ago] we had just scrapes off the table from Engineering but as the pressure increased [due to an increased product portfolio] to fix more and more problems they had to give us the information we needed to alleviate their workload. [As a result we have] taken over more and more and more of the responsibility of the product after it has gone G.A". Knowledge [design specifications and bugs] regarding a new product is a valuable asset and a significant "risk if competitors can get a hold of it and reverse-engineer it and then be the first to market", as stated by the Operations Manager. As described by the Engineering Manager, "depending on where it [new product] is in the product life cycle [specifically G.A] we would share as much information as we can with Sales to help them understand the product but we don't want information [regarding a new version] released before it's ready to market".

Inter-relationships "with customers is vital for our group; they are considered a key source of knowledge [regarding] our products which is collected by tracking calls [Power-Link] and through face-to-face meeting in the Executive Briefing Centre", as stated by the Knowledge Consultant. "We also have a good collaborative relationship with fifty or more vendors for technical documentation", according to the Engineering Trainer.

Knowledge resides in several reservoirs within the organisation, which are summarised in Table 5.5.

CUSTOMER SUPPORT FUNCTIONS: RESERVOIRS OF KNOWLEDGE	
People:	
Individuals	• CS Specialists (Table 5.2 provides an overview of the different experts within the case) Network of experts/problem-solving for Customer Calls or fixes • Engineers – Product designs, fixes and debugging • CS Manager – CS Coordination & Procedures • Knowledge Consultant – centralising data, information and knowledge • KDG Officer – Developing Subsidiary Skill sets • Knowledge Champion – KM Practices
Groups	• Management Forum– policy issues • Engineering – U.S./Cork, Ireland • KDG Corporate Group – KM Strategy for CS • GIS/IT Department – IT Services and guidelines • Customers – Feedback/Reviews (or evaluations) • Executive Briefing Centre (Cork)
Artefacts	
Procedures	• Templates for Solutions • Call Escalation Procedures
Repositories	• Vendor repositories • Knowledge-Link for Online Training • Documentation of Solutions • Managers Discussion Forum • Channel CME-Co (Intranet) – Corporate Information and group specific websites • Power-Link • Engineering Alerts • Engineering Bug Tracking System
Technologies	• Primus – Call tracking
Org. Entities	
Organisation	• KM Infrastructure (Table 5.3 provides an overview of the organisations knowledge)
Units	• Engineering • Research & Development • Sales • Executive Briefing Centre
Inter-organisational Relationships	• Customers (stakeholders) – advice regarding products Access product solutions through Power-Link • Partners (vendors) – joint expertise in providing solutions/requirements Access through E-Room and face to face meeting

Table 5.5: Reservoirs of Customer Support Knowledge.

5.1.3.3 Customer Support KM Processes

This section describes the processes used to support the acquisition, capture, creation, sharing, application and control of knowledge in the CS function.

The **acquisition** of knowledge within CME-Co is common. As described by the Knowledge Consultant, "Documentum was bought so that departments could collaborate with customers, partners and suppliers. We are also trying to encourage CS groups to use the platform for storing their own information and knowledge". "IT and ISS allocate controls once our customers register to use E-Room and Power-Link so that they can't access sensitive information and employees can decide who [internally] they want to access their own documents", as stated by the KDG Officer. As explained by the IT Manager, "we maintain the different applications and systems used by CS; if information sharing [access] is required we [IT] escalate the problem to the assigned Security Officer". "We use NDA[14]s and we have the capability of tracking what they [customers, suppliers and competitors] do as everything on our network is tracked. But we would typically limit what they can do, so if someone is coming in to get access to the Clarify [the call-logging] system, we would tunnel [using a VPN] their connection to Clarify or to our ERP system", as explained by the [Cork] Security Officer. "The firewall rule-base is also regularly checked to block or unblock CS access to [vendor] sites for warning emails or White Papers", as stated by the [Cork] Security Officer. "Usually they [CS] tend to bypass some [of our] controls if they want to download something like a web crawler, scanning tools or how to guides, making our [ISS's] lives difficult if a virus bypasses the DMZ and disrupts the [Corporate] network", as explained by the [Cork] Security Officer.

Knowledge is **captured** or retrieved from the numerous reservoirs distributed throughout the case organisation (sub-section 5.1.4.2). As explained by the KMS Administrator, "Primus enables the availability of the collective knowledge of CS to the different end-users so that problems are solved quickly". "A knowledge worker in Hopkinton can easily use a solution constructed by an expert in Sydney. The capture of knowledge pertaining to: problems, customer queries and tracking the frequency of occurrences enables focused product improvements", as stated by the Knowledge Consultant. "They [CS] look for feedback from customers regarding the problem as well as stats from Primus to improve productivity", as stated by the KDG Officer. The CS Manager explained that, "if a solution is continually reused, Engineering can examine the root cause and fix new releases of the product". "Search capabilities and queries allow us to retrieve stats for proof of the value of creating solutions and analysing their reuse", as stated by the KMS Engineering Trainer.

Knowledge is continuously **created** through the problem-solving process used within CS. As described by the KMS Engineering Trainer, "the escalation process used in CS is the approach used to manage or resolve calls [to create solutions]". "Customers are encouraged to open a ticket, through Clarify, to all of their vendors [an environment could have many platforms] so that different platforms and system Engineers can collaborate", as stated by the CS Manager. "If a problem isn't resolved by the customer or the field Engineer onsite it is escalated to CS. The CS Technician takes the call first and then if he or she can't cancel the problem it is escalated to Level 1 Support [product

[14] A non-disclosure agreement (NDA) is a legal contract between at least two parties that outlines confidentiality material, knowledge, or information that the parties wish to share with one another but wish to restrict access to thirst parties.

support Engineers and Software Analysts]. If it's not fixed the problem is then raised to Tech Support Level 2 along with the work done [through Clarify, phone calls and Primus]. If Level 2 can't fix the problem it goes to Design Engineering in the States", as explained by the Level 2 Engineer. As described by the Knowledge Consultant "we have found historically that any resources involved [through the escalation process], such as: time personnel, Finance, the cost just goes through the roof".

CS **shares** knowledge through its problem-solving processes. "Solutions are: created, stored, shared and used through our KMS [Primus]", as stated by the CS Manager. However, according to the KMS Engineering Trainer, "Field Engineers would be more effective if they could pool their knowledge together. A Field Engineer in Japan has no interaction with a field Engineer in Germany, France or the U.K. There seems to be a hang-up about this group's technical ability and lack of knowledge regarding projects so they cannot share their knowledge or access the same solutions as CS Technicians". Even though Field Engineers "would be more productive and reduce our [CS] calls they are blocked from even working together", as stated by the CS Manager.

As described by the Knowledge Consultant, "a lot of knowledge transfer is built on barstools talking about problems [calls] and building relationships, but if someone leaves that relationship ends. Unless you have certain service level agreements between functional groups there are restrictions on what they [U.S. Engineering] will share".

Feedback from customers suggests that "they are happy with vendors who share everything so that nothing is hidden from them. CME-Co utilises a priority mechanism that allows customers to tag a problem in Power-Link as urgent and we deal with it straight away. We also share revisions of fixed bugs. We are able to draw up the lists of all the customers who are affected by known bugs because they have registered their software and their revision software and we are able to find out which customers have the affected product", as explained by the KMS Engineering Trainer. The CS Manager stated that by "pushing knowledge back towards our customers, customers can help themselves to fix product issues without calling us, reducing the burden on the support organisation. Giving them more and more access allows them to fix their own problems".

Knowledge is **applied** throughout the escalation process. As explained by the KMS Engineering Trainer the "product portfolio is so wide and complex that you can't expect any one individual to be able to support them all so we document solutions of problems and this increases productivity as the Primus tool allows to reuse existing solutions and save the next Engineer from going through a debug procedure". As described by the CS Manager, "if a solution is continually reused, Engineering can examine the root cause and fix new releases of the product". Additionally, according to the KDG Officer, "the system is used as a training tool and has dramatically reduced the time to get Engineers up to speed in three to four months, a reduction from the six months reported prior to the introduction of the system", freeing senior staff for more complex issues and making inexperienced staff more self sufficient.

Knowledge **control** is necessary to assure the validity and utility of knowledge. As described by the KDG Officer, "access to our knowledge repositories such as E-Room and Primus is restricted to various groups for the time being as there is some information that [Management] don't want out there". "A quality mechanism is used to ensure that new products, new designs are kept at management level until a product meeting is arranged and access [to technical design and bugs] is then discussed", as

stated by the Engineering Trainer. "The level of access to the KMS solution [Primus] is controlled by Engineering to assure the confidentiality, availability and integrity of product designs and bugs", as stated by the Engineering Manager.

The release of solutions or fixes is strictly controlled. Engineering control the process due to risks such as "reverse-engineering, new version release dates and improvements [fear that Sales will inform customers], release of known deficiencies in the code [affecting sales] and the inexperienced application of the debugging procedures and commands by some levels of Support", as stated by the Engineering Manager. As explained by the CS Manager, "security comes into play when a fix involves issuing privileged commands to a product that is potentially a dangerous command. Some commands could completely screw up a network configuration or destroy data. There's an obvious reluctance to make these available to customers and that is something that we want to keep to ourselves". However, according to the Knowledge Consultant, "ninety-nine percent of the time nothing goes wrong so customers could and should have access to everything".

As described by the KMS Engineering Trainer, "CS should have full access, sometimes it feels like we are working in different companies and we need access to their [bug tracking] systems". "Access seems to be based on domain access rights [15]– for example an Engineering student working in the States for an internship would have access to their [Engineering] systems. I worked as an Engineer here for thirteen years and I still can't get access to solutions or bugs that I am more than capable of using correctly", as stated by the Knowledge Consultant. Access is tightly controlled and according to the CS Manager "we would ultimately like access to the source code for the products, a few of our Engineers here [Cork] are technically skilled to use that information. Access to their bug tracking system would be very beneficial so that we could search to see if Engineering has already solved a bug logged by a customer to CS. It is frustrating for us to spend time working on a problem and to discover, when it's escalated to Engineering, that they were aware of the problem and had the fix which could have cost us a week in time and resources".

As explained by the KMS Engineering Trainer, "they're very few official security restrictions in place; usually controls are allocated based on the requirements of individual departments. IT and Security work with PPMG to collect requirements and allocate the necessary support". "Primus solutions have both solution security and basement level security, which is a four level security model is currently being used [it used to be ten levels]. The least secure level would be a product where anyone that has access to the Internet could view those solutions. The next level is the customer with access to fifty percent of our solutions through Power-Link. The third level is support and the highest level of security [access] which would be heavily restricted and accessible through Engineering and selected personnel", as explained by the KMS Administrator. According to the IT Manager, "access rights are very much a challenge for us when users, particularly CS, feel that they should have access to certain information. But most recognise that we are just doing our jobs and Engineering is a law unto them-selves".

Table 5.6 summarises the Customer Support KM processes identified within CME-Co.

[15] Domain access rights are used to describe the access rights assigned to a networking workgroup.

CUSTOMER SUPPORT FUNCTIONS: KM PROCESSES	
Processes	
Acquisition	• Purchased Documentum – to utilise collaborate SW (e-Room) for joint projects with Vendors, Partners and Customers • Reverse-engineering – competitor and vendor products for debugging • Subscription to Technical Groups – Manuals, Procedures, Updates and Tools
Capture	• CME-Co Reservoirs of Knowledge (Table 5.8) • Pool of Experts – through the problem-solving process • Roles and responsibilities – for escalation • Solutions retrieved through Primus
Creation	• Problem-solving Process – for the creation of a solution • Escalation Process – for the collective creation of a solution • Collaborating with Vendors for solution generation • Lessons-learned – as a result of creating a fix
Sharing	• Problem-solving – Sharing knowledge to solve and problem or fix • Collaborating with each CS Level • Collaborating with partners
Application	• Reuse of customised solutions for products • Knowledge reused from a previous escalation • Reuse of solutions through Primus and Reuse of knowledge from the debugging process • Pool of Experts – use develops through trading
Control	• Acquisition of external knowledge is tracked • Quality mechanisms are utilised • Level of Access to Primus (solutions) is controlled by Engineering • Restricted control of commands • Domain specific controls • PPMG Mechanism for identifying unit requirements (access)

Table 5.6: Customer Support KM Processes.

The next section describes ISS function's approach to managing knowledge.

5.1.4 IS Security Function

The Global IS (GIS) and IS Security functions are, according to the Corporate Security Coordinator, "separate yet interdependent". The IS function within CME-Co is described by the CS Manager as "a supporting organisation globally and locally [Cork]". Structurally CME-Co has divided the ISS function, according to the Security Officer, "into four autonomous units under the GIS umbrella with the same reporting structure". GIS is the primary corporate IS department based in Hopkinton and a separate IS department supports CME-Co International. CME-Co International refers to any operations based outside of North America. It is EMEA (Europe, Middle East and Africa) and Asia and Australia. As explained by the IT Manager, "the IS department is a value-added business support function", providing IT services for all of the groups within CME-Co International. The [Cork] IS department, according to the Corporate Security Coordinator, "reports to and collaborates with Corporate GIS". The mission of Global IS (GIS) is, according to the Compliance Coordinator, "to enhance productivity and knowledge enablement across CME-Co by proactively delivering and supporting innovative, world class business solutions, infrastructure and operations".

The IS function collaborates with and services the International Finance group, Sales and Customer Support function and importantly the global IS Security function. The GIS function operates closely with the Customer Support function which supports the CME-Co product portfolio. The two functions use a version of M-Gates for joint

projects so that collaborative projects are recorded efficiently, and responsibility (an employee) is assigned for stage deliverables. The customer base for the department, according to the IT Manager, "is twenty thousand CME-Co International business users". These include Customer Support Engineers, sales representatives, manufacturing plants and Engineers. In order to support user needs the GIS function utilises, as stated by the IT Manager, "a portfolio group which is the group that interfaces between the IT function and the business functions through account managers [from the specific business functions] to ensure that what we're delivering [and] doing is correct for the business". Close to a hundred people are employed in the IS department with the primary objective of delivering IT services for the international business function of CME-Co.

The IS department has always been considered part of the overall corporate GIS group. Due to its relatively small size in comparison to GIS, the department's structure is, according to the Infrastructure Manager, "simple and the members are highly and broadly skilled with needed flexibility". As explained by the IT Manager the local IS group allocated IT staff to "the international business functions on the portfolio side and a number of people here in the various functions within IT for application development, network [NW] and security, servers and the data centre". The IT Manager also stated that locally security is separated into "internal versus external access, external access to the CME-Co corporate network and applications through user accounts and passwords". IS Security is managed locally by a Security Officer who, according to the Corporate Security Coordinator, "works as part of the IS function reporting to the IT Manager in addition to the Corporate Security Group. The Security Officer is responsible for enforcing corporate policy [such as ISO17799] regarding security and compliance".

The IS Security function within CME-Co is separate from GIS but reports to the Global IS Director in the U.S. who, according to both the IT Manager and Corporate Security Coordinator, "reports to the Chief Information Officer who in turn reports to the Chief Financial Officer". Security is divided into two fundamental groups operating within corporate headquarters and dispersed throughout the multinational. The Corporate Security Group is according to the corporate security coordinator "a representation of a group of stakeholders [customers, partners, and regulatory bodies] and what it is that they want to do with security and make it [their requirements] part of the corporate security plan". The function, as stated by the [Cork] Security Officer, "focuses on working with Design Engineers in enhancing CME-Co products with security tools". Therefore, as stated by the Corporate Security Officer, "we can make our products more competitive and differentiate them by using security as a differentiator, in meeting customer requirements, and providing a new business opportunity for CME-Co".

As described by the Corporate Security Coordinator, "Corporate officers are used to ensure compliance and the group also has quarterly compliance reviews as part of our SEC[16] quarterly filings. The Finance department and the Legal department both focus intensively on meeting those requirements in conjunction, of course, with external advisors and bodies like our audit committee and our external auditors and other advisory consultants". The Corporate Security group is, according to the IT Manager, "a small group; there are eight people; it is a cross-functional team; you could say that it is a strategy-development team". The group is as stated by the Corporate Security Coordinator "an effort on our part to make security just a part of what it is we do, so it is

[16] An SEC quarterly filing is a financial statement submitted to the U.S. Securities and Exchange Commission (SEC). Public companies are required to make regular SEC filings. This information is used by investors for investment evaluations.

not unique or special, it is just something that we pursue as part of our regular engineering activities [and] as part of product development activities, customer engagement activities, when we are deploying them in the field to demystify security and make it part of the company's infrastructure".

Finally the OISRM is the Global ISS function within CME-Co. It is an internal facing function and uses Security Officers dispersed throughout the different subsidiaries. As described by the OISRM Coordinator it is concerned with "making security a part of the technologies that we use internally, and similarly on the product side optimise the use of security for our Engineering folks and for the tools that people are using in the field". Additionally the Corporate Security group is responsible for "identifying the different requirements of our stakeholders which are CME-Co customers", as stated by the Corporate Security Officer. The OISRM is also, according to the IT Manager, "responsible for identifying security standards, implementing security and managing security breaches". The group does interact with the GIS and IS departments in coordinating the "rolling out of virus software and collaborations with partners such as McAfee and Microsoft".

The next section identifies and describes the different types of knowledge utilised by CME-Co's ISS function.

5.1.4.1 Types of ISS Knowledge

The different types of ISS knowledge are described in the next three sub-sections. The first section describes the general knowledge necessary for the ISS function practitioners to conduct their day-to-day operations. Sub-section 5.1.2.2 and section 5.1.4 described the reporting structure of the organisation and the ISS function itself, which is regarded as fundamental knowledge in allocating roles and responsibilities at corporate and local (subsidiary) levels.

General knowledge common to the ISS function is varied. As explained by the IT Manager the management of IS Security is a knowledge intensive activity and "multiple sources like standards and security technologies are used [and regarded] as security knowledge". Everyone in IT, IS Security and Customer Support, according to the [Cork] Security Officer "knows how to search Channel CME-Co [the Intranet] for specification docs if there is a problem with a proxy server, firewalls, scanning tools or search Microsoft for patch guidelines". The majority of the ISS interviewees stated that external sources such as: "Microsoft and McAfee [vendors] threat warnings are vital". The knowledge of possible impacts due to threats like viruses is also regarded as fundamental. According to the Security Officer, "if a virus brings down a high priority port[17] – it could cost us a lot of money and potentially customers– depending on the downtime". As explained by the Corporate Security Officer a basic knowledge of regulations impacting the organisation is vital as "CME-Co like so many other companies needs to understand the different regulations out there". Additionally collaborative projects, through the portfolio management system, must utilise the corporate project management methodology. As explained by the IT Manager, "M-Gates is used by everyone so that the same steps are followed no matter what the project is – the more projects you're assigned to, the easier it [project management] becomes".

[17] A port in a TCP/IP (Transmission Control Protocol/ Internet Protocol) network is an endpoint to a logical connection. The port number identifies what type of port it is. Port 80 is used for HTTP (Hyper Text Transfer Protocol) traffic accessing, for example, corporate web services.

The next sub-section describes the technical ISS knowledge utilised by members of the ISS function.

Technically specific knowledge is specific to the ISS function. At a strategic level CME-Co identified security and regulatory issues as key customer requirements. The Corporate Security group was formed, as stated by the Group Officer, to "determine the needs of the different stakeholders and map those needs to the strategy of the company". As a result documents describing IT and ISS regulations "are a vital source of reading to aid in outlining the steps needed to adhere to regulations such as SOX", as further explained by the Compliance Officer. The security policy refers to the set of rules, and practices which regulate how CME-Co manages, protects and allocates its resources. "The [ISS] policy is available to everyone but IT and Security must implement it", as stated by the IT Manager. The principles of security are documented in the ISO17799 guideline which according to the Corporate Security Officer is "like the U.S. Constitution which is a two hundred year document". The fundamental principles of the document itself continue "to apply regardless of changes in technology". The ISO17799 requires confidentiality, integrity and availability (C.I.A) and, according to the [Cork] Security Officer, "is a type of document which gives you continuing requirements that are likely to be relevant ten years from now as they are today". The organisation also keeps ahead of technological changes in the market "by playing a role in the development of the protocols", as stated by the [U.S.] Security Officer. As described by the Corporate Security Officer, "CME-Co is represented on the various standards setting bodies involving protocols that impact storage and storage security".

Security technologies are also a source of technically specific knowledge. According to the [Cork] Security Officer, "log files from firewalls are useful, but you need experience in differentiating between real threats and everyday annoyances". Experience in analysing the behaviour of traffic and alerts "is the only way to filter out the endless lists and prioritise [activities]", as further explained by the Remote Access Coordinator. Knowledge of the business side of the organisation is fundamental to day-to-day operations as, according to the [Cork] Security Officer "it helps us [IS Security] to identify priority systems and apply the right controls to the different servers and for example the engineering databases". The ISS function also relies on this general knowledge and feedback from departmental managers to, according to the IT Manager, "allocate the right access to the right users".

The next sub-section describes the knowledge used for a particular circumstance or project.

Contextually specific knowledge within the ISS function of CME-Co is primarily used to adhere to regulatory issues or for an incident such as a security breach. As described by the Corporate Security Officer the company is, "involved with the different regulatory agencies themselves that define what the protocols are going to be, developing new technologies, filing patents ourselves and just I would say trying to hire new people all of the time and training people. These are the ways that you stay ahead if you can of those market dynamics".

External explicit and tacit knowledge is also sourced for use by the function. As explained by the [U.S.] Compliance Officer "we use material such as White Papers on SOX, recommended, risk analysis models, audit reports from Deloitte and in-house training manuals for SETA". The Compliance Officer further explained that it is the "[ISS] members who then apply these guidelines to make sure we [CME-Co] are

compliant and learn from each audit". The company also utilises the knowledge gained from audits to create relevant training for specific functions. As explained by the Compliance Coordinator, "if we can we will train the different members of the security and IT functions and our Design Engineers in regulatory issues to reduce the duration of audits and incorporate security enhancements into our products".

Unexpected incidents, such as security breaches, according to the Compliance Coordinator, "generally result in reactive measures". Incident response teams are formed from specific areas and utilise "steps customised and outlined in the ISO17799 document", as described by the [Cork] Security Officer. Feedback from auditors is also used to identify "weaknesses in our security network – so we will generally take steps to rectify these", as explained by the [Australian] Security Officer.

The different types of ISS knowledge identified within the organisation are summarised in Table 5.7.

IS SECURITY FUNCTIONS: SECURITY KNOWLEDGE						
Types	**General Knowledge**	**Role**	**Technically Specific**	**Role**	**Contextually Specific**	**Role**
Declarative						
Explicit	Documentation describing: CME-Co, Stock options	O	A document describing IT & ISS Regulations	S	A White Paper describing the IT /ISS requirements for Sarbanes-and-Oxley	O
	Organisational Chart: outlining the internal reporting structure	O	A document describing the multinationals security policy	S	Risk analysis documentation: outlining procedures for ID Risks to the Org.	O
	IT Specifications for Servers, IDS, Firewalls & Virus Software	O	Access control lists: for Domain (function) access & Segregation of Duties	O	ISS Audit reports: containing evaluation of Security Infrastructure	T
	Vendor threat email warnings	O	A document describing the ISS Strategy	S	SETA Training manuals: updated to include improvements	O
			Alert Reports from Security Technologies	O		
Tacit	Knowledge of the Regulations pertaining to CME-Co	O	Knowledge of the factors to consider when implementing regulatory requirements	T	Compliance officers knowledge of Sarbanes-and-Oxley requirements	T
	Knowledge of impact of the different possible threats	O	Knowledge of the factors to consider when advising CME-Co customers on ISS issues	S	Security Officers knowledge of different risks and vulnerabilities	T
	Knowledge of functional experts & escalation levels	O	Knowledge of Domain (Function) access requirements	O	Compliance Coordinators knowledge of ISS Audit issues that may arise	T
	Knowledge of CME-Co roles & responsibilities	O	Knowledge of the priority systems in CME-Co: to align to Controls	T	Compliance Coordinators knowledge of regulatory issues to include in SETA	O
			Security Officers knowledge of risks	T	Case (Problem & Solution)	O
Procedural						
Explicit	A White Paper describing the steps in aligning Security Controls to internal projects	O	ISO17799 – section describing, for e.g., Disaster Recovery procedures for a Web Server	T	ISO17799 document identifying the sequence of steps a response team should take in the event of a security breach	T
			Manual describing Firewall alert indicators	O	Auditors Feedback report identifying issues to address and Network (NW) test reports	T
Tacit	Basic knowledge of the steps necessary to align IT to internal projects	O	Security Functions knowledge in developing a security plan/strategy	S	A Security Officer's knowledge of steps to take in the event of an incident	T
	Basic knowledge of the steps needed to create an up-to-date End user lists	O	Security Functions knowledge of the steps necessary to protect the organisation	T	A Security Officer's knowledge of steps to take to prepare for an Audit	T
			Security functions knowledge of the steps necessary to block an attack	T	Compliance Coordinators" knowledge of the steps to take in addressing audits	T
* Knowledge Roles: Operational = O; Tactical = T and Strategic = S						

Table 5.7: Types of IS Security Knowledge.

5.1.4.2.1 Reservoirs of IS Security Knowledge

Knowledge, pertaining to the CME-Co ISS function, resides in several different locations within the organisation. They encompass people and functions, including, IT and Security professionals, Engineers, management and functions/teams within ISS. Artefacts, including best practices, security technologies, and repositories are used. Organisational entities, including organisational units, organisations, and inter-organisational networks are also sources of knowledge. The organisation itself, in its entirety, is a knowledge reservoir. The norms, values, structures, practices and culture are contextually specific knowledge. This reservoir of knowledge is described as part of the organisational infrastructure in section 5.1.2. The remaining reservoirs of knowledge are discussed in the rest of this section.

A considerable amount of knowledge resides in **people**. As explained by the Corporate Security Officer, "security is a process that depends heavily on the expertise of [individuals] Security Officers, IT staff, and employees in general". He further explained that "it's who you know that counts – if you have a problem, you need to know who to go to". However, according to the Compliance Coordinator, policies are more important than experts "it's more policies as opposed to going to a Security Officer – everything needed is outlined in the [ISS] policy". According to the [Cork] Security Officer, "there's a pool of people in the U.S. that I would go but there are problems getting that knowledge from them when I need it because it's a different time zone, they are five hours behind us". He further stated that a list of contacts is vital for his role "I have my own table of contacts for every system under the sun". "It's not a HR system by any means. It's my own personal system because at the end of the day there's literally in total [of] maybe twenty critical people, who are [based] in the U.S., for the various systems". At a management level the IT Manager stated that "it is the Global IS Director's, in the U.S., sole job is the security of systems and to find security standards, implement security plans and manage security breaches [by coordinating incident response teams]".

The structure of the **groups**/teams working within the ISS function is described in section 5.1.4. The different groups, including OISRM, the Corporate Security group, GIS, the [Cork] IS department and Remote Services operate individually and collectively. As described by the Corporate Security Officer, "the OISRM identifies [security] risks for CME-Co, selects and advices the different subsidiaries [through the onsite Security Officers] regarding the best practices for allocating appropriate controls". The OISRM is a source of contact [expertise] regarding "the compliance aspect of our organisation [we can] go to the group to address a security issue or a policy issue or a process issue which could have a compliance or a security impact", as stated by the [Australian] Security Officer.

The Corporate Security group is, according to the IT Manager, "[a] strategy and development group, making security a part of their regular engineering activities as part of product development activities and customer engagement activities when deploying them [products] in the field". In turn the IS department, under the umbrella of GIS "is responsible for rolling out IT services to address the requirements of the different business functions as identified by the portfolio managers", as stated by the Infrastructure Manager. As explained by the [Cork] Security Officer "we have a number of people in IT who would have a lot of knowledge of security even though it wouldn't

be their primary role – it would be a main area of focus, around virus protection and [Network] monitoring. We [Cork] can roll out a security patch to all of the PCs within twenty-four hours. [However] we have had instances in the last eighteen months where we have had to upgrade every single server in our network – thousands of servers". The Compliance Officer stated that the organisation "has very strong internal controls and was recognised by the SEC [as such]. So we do have Corporate Officers whose job it is to ensure compliance and we do have quarterly compliance reviews as part of our SEC quarterly filings". The Finance department and the Legal department focus intensively on meeting those requirements in conjunction of course with external advisors and bodies like the audit committee, external auditors and other advisory consultants. "The Remote Services group enables internal and external access based on the requirements of the different domains and the different stakeholders", as stated by the Remote Services Coordinator. This knowledge is combined to create a substantial pool of expertise.

Knowledge is **stored** in **artefacts** such as practices, technologies and repositories. **Practices** can be organisational routines and procedures. As explained by the Corporate Security Officer, "compliance procedures outline the steps needed in order to comply with whichever law is being prioritised by management". Due to the nature of the environment the organisation is operating in "CME-Co is subject to U.S. and international laws", as explained by the OISRM Coordinator. "Regulatory procedures list in sequence the steps IT and ISS must take to comply with the regulations of the countries we are operating in", as stated by the Compliance Officer. CME-Co's ISS procedures have been developed over time through "good and bad experiences", as explained by the Security Officer. As described by the IT Manager "we document solutions as much as possible – so that we can solve problems faster and have a source for new staff coming in. One of the global initiatives which have impacted us is Sarbanes-and-Oxley; we have just implemented a whole series of procedures to support the SOX requirements in the U.S".

The ISS function stores these procedures in repositories, as stated by the [Cork] Security Officer, "we either store solutions, procedures and guides [for example a customised ISO17799 document] in our shared drives, Channel CME-Co, the OISRM website or Primus [a CBR tool]". As described by the [Australian] Security Officer, "we wouldn't know what fixes [patches or procedures] Cork or the U.K have unless we checked the internal Security [function] websites". He further stated that, "the OISRM online source material [procedures] is vital for us – they [OISRM] direct all of the different Security Officers regarding regulations and policies". As explained by the IT Manager, "IT and Security [members and groups] know that we all benefit if we store our security procedures in the group drives". He further explained that, "there is a drive led by X [the Knowledge Consultant] to centralise our knowledge and share it – it's no use stored on our desktops". Vendor sites are also considered invaluable as a source of documented procedures for "security technologies like our VPN [Virtual Private Network] installations, SID [Secure ID], monitoring tools [administrator software] for our firewalls and proxy servers in our corporate network and our IDS [Intrusion Detection Software]", as stated by the [Cork] Security Officer. According to the Corporate Security Officer, "there are online repositories of knowledge so if Security [experts] have a compliance issue or were wondering if a solution [found online] should be used in a particular way there are processes [procedures available] in place which facilitate resolving those issues [problems]". As explained by the [Australian] Security

Officer, "there are also portals and a global tech web [site] which is basically [a group of online] file servers that store all the random patches of the time and various bodies [procedures and standards] of information".

A considerable amount of knowledge is stored in CME-Co **technologies** and systems. Primus is used to store solutions for IT and Security problems. As described by the [Cork] Security Officer, "we [Security Officers] try to use it [the CS KMS solution] as much as possible to track problems and for escalations as it's designed for that – but time wise it's difficult to document a quality solution sometimes". Primus is used to track calls [from employees] but adding solutions "when if it's a difficult call – up to three or four levels of ISS Technicians and [Security] Officers could be involved and it's hard to make sure everyone does it" as stated by the IT Manager. As stated by the Corporate Security Officer, "every attempt is made to use centralised shares and technologies so that work isn't duplicated". Email is also used to store tacit and explicit knowledge as security members "often solve a call through email" as stated by the [Australian] Security Officer. As described by the [U.S.] Security Officer, "it's [MS Outlook] a convenient tool to use, it's fast and easy to unofficially use, but cleaning and managing the solutions is difficult – email can be a filtering nightmare".

Knowledge is also stored within **organisational entities**. These range from the entire organisation, units within the organisation and inter-organisational relationships. The organisation as a whole is described in section 5.1.2. The culture, structure, values and practices are discussed and summarised in Table 5.3. As explained by the Corporate Security Officer, "CME-Co is [very much] dependent on [**inter-**] **relationships** with customers; partners and we even work with our competitors". He further stated that, "customers are basically the advisory group that you [CME-Co] want to pay most attention to, insofar as you want to stay ahead of their needs". As stated by the Briefing Centre Manager, "[CME-Co] listens carefully [to customers] in order to build their requirements, such as security, support, storage for regulatory needs, into the corporate roadmap". As described by the Corporate Security Officer, "you're probably at a greater risk by not working with them [customers]". He also stated that "an organisation wants to be the advisor that customers go to rather than your competitor". Customers can also access technical knowledge regarding the different corporate products "through Power-Link [Extranet] which is our [customer] portal to the Primus system" as stated by the [Cork] Security Officer. He also added that their access is limited to "fixes approved by our Engineering group and some of the Level 2 Technicians here".

Vendors are also considered valuable sources of knowledge and collaborators in joint projects. As explained by the [U.S.] Security Coordinator, "we would suggest that the customer open up a ticket to all the vendors involved and then we would collaborate with specific Engineers once the incident was assigned to an Engineer within another company". CME-Co has a relationship with "fifty or more vendors", as stated by the Corporate Security Officer. Suppliers are also considered a valuable source of knowledge. As described by the IT Manager, "CME-Co bought a company, Documentum, who specialise in E-rooms, to collaborate with suppliers [for example Dell] and exchange [customer] feedback about products, changes in the market and potential time saving initiatives". The organisation also collaborates with competitors through regulatory bodies "on all of the [security and regulatory] standards" according to the OISRM Coordinator. He, as well as the Corporate Security Officer, further explained that "when you are supporting common standards that facilitate

interoperability you have no other choice but to work with competitors". External consultants are utilised to analyse the effectiveness of the controls in place and according to the Infrastructure Manager "audit our IT Infrastructure [by] performing penetration tests, review access control lists and anything else needed for SOX". Even though this is generally "a time-intensive process" the knowledge gained as a result is, as stated by the Corporate Security Officer, "useful and informative for the next review".

The ISS function also collaborates with other functions within CME-Co. As described by the IT Manager, "during the initial phase [of the M-Gates methodology] when we were trying to solve a common problem a dedicated team is put together with representatives from every single major function such as Hardware Engineering, Software Engineering, Customer Support, Marketing and Finance to build a business case [for a proposed initiative] and if approved the project will go ahead with a bigger and a more dedicated team". As explained by the Security Coordinator, "each function has their own requirements and skill-sets for a project and must provide details regarding their functions access [rights] requirements to us [ISS]". This knowledge is domain or unit specific and dictates individual and group access to CME-Co's knowledge stocks as specified by management and "due to SOX the Finance department", as stated by the Corporate Security Officer.

Knowledge resides in several reservoirs, which are summarised in Table 5.8.

IS SECURITY FUNCTIONS: RESERVOIRS OF KNOWLEDGE	
People:	
Individuals	• ISS Specialists (Table 5.2) – network of experts/problem-solving for critical systems • Engineers – Product designs, fixes and enhancements (security) • GIS Director – Best standards • Site Security Officer – Implementing Controls • Corporate Security Officer – compliance issues and stakeholder requirements
Groups	• Management – Policy issues pertaining to standards & procedures • OISRM – Pool of experts regarding: standards and best practices • Corporate Security - strategies and development initiatives • IT Department – IT Services and guidelines • Security Officers – Domain Knowledge • Audit Committee - Compliance issues, internal reviews and guides • Remote Services – external access requirements
Artefacts	
Procedures	• Compliance procedures – U.S. and International • Six Sigma – Business Case Resource Requirements • M-Gates – phased approach to project management incorporating checklists
Repositories	• Documentation - IT /Security solutions or fixes • Shared Drives – solutions, procedures and guidelines (e.g. ISO17799) • Channel CME-Co (Intranet) – Corporate Information and group specific websites • Desktops /Portals – E-Room and Power-Link • Global Tech Web/File Servers – External sources of patches and solutions • Question & Answer Repositories – Security Queries, for e.g. Compliance • Vendor Sites – Manuals, Installation Guides
Technologies	• Primus – Call tracking • MS Outlook – Problem-solving but filtering/retrieving the knowledge stored is difficult. • VPN – Secure external traffic| SID (Secure ID) – Access logs of employee system use. • Monitoring Tools – Alert logs of failed & successful system access • Firewalls & IDS – Alert logs for internal & external access | tracking
Org. Entities	
Organisation	• Organisational Infrastructure (Table 5.3: an overview of the organisations knowledge)
Units	• Joint Projects – Domain specific requirements for X project • Other functions - Domain requirements & access, roles & responsibilities, systems. • Finance – Access requirements to corporate knowledge stocks • Portfolio Project Management Group (PPMG)
Inter-organisational Relationships	• Customers (stakeholders) – advice regarding products, requirements and Corp goals. • Access product solutions through Power-Link • Partners (vendors) – joint expertise in providing customer solutions/requirements • Competitors – standards and interoperability agreements • Auditors – Reviews, lessons-learned and guides

Table 5.8: Reservoirs of IS Security Knowledge.

5.1.4.3 IS Security KM Processes

This section describes the processes used to support the acquisition, capture, creation, sharing, application and control of knowledge in the CME-Co ISS function.

The **acquisition** of knowledge within CME-Co is common (Table 5.1). As explained by the Corporate Security Officer, "it is necessary in order to stay ahead of the competition". "We [ISS function] bought Documentum so that we could facilitate a secure connection, in the case of the company, with our customers, suppliers but also with our vendors [McAfee and Microsoft] so that we could collaborate more effectively", as stated by the IT Manager. As described by the OISRM Coordinator, "regulatory guidelines, step-by-step procedures for standards and security frameworks are purchased or licensed so that we are compliant". The knowledge required to develop market standards and security procedures is enormous and according to the Corporate Security Officer, "impossible to produce internally, agreement is obviously needed across the industry regarding interoperability of products and [security] practices are developed and tested by regulatory bodies so obviously we purchase this knowledge". The organisation, through the relevant function, will customise this acquired knowledge "to suit the environment we operate in", as explained by the [Cork] Security Officer. External consultants such as J.P. Morgan are used to audit the controls and procedures internal to the organisation. As described by the GIS Director, "auditors are employed because we are legally required to comply with regulations to remain listed on the Dow Jones. They do also provide us with valuable reviews of our controls and advice regarding segregation of duties". "Design Engineering reverse-engineer our competitors products and we [ISS] customise standards like ISO177 99", as stated by the OISRM Coordinator.

As explained by the [U.S.] Security Officer, "we pay a type of subscription to public technical support groups for [administration] manuals, recovery procedures, updates – anything we need we source externally or one of our vendors provide us with updates or tools". The IT Manager stated that, "it takes about six months for new employees to become useful, but we are getting better at speeding things up by providing tutorials on things like SOX". CME-Co provides "extensive training programmes throughout the different GEO's [subsidiaries] using Knowledge-Link". CME-Co employees can register for and participate in online training tutorials through Knowledge-Link, a training portal. "Tutorials are designed and customised for CME-Co, employees go through them online and a record is kept with employee profiles and other data repositories that the company uses", as stated by the Corporate Security Officer. "Security specialists are also outsourced from security vendors for specific projects to reduce project life cycles or to ensure new security technologies are implemented or maintained correctly", as stated by the [Cork] Security Officer. Vendors perform ongoing tests of their products to ensure that they can counteract evolving threats. Vendors provide "patch updates as part of their contracts with their customers – it's impossible to provide or buy security tools that cannot eventually be bypassed", as stated by the [U.S.] Security Coordinator. As explained by the Corporate Security Officer "the rights to off-the-shelf [for e.g.] encryption products are bought and developed further internally". He further explained that the Corporate Security group, as part of its development strategy, acquire "source code and all the rest of it to meet the requirements of our customer". As described by the Remote Services Manager "rapid remote was a product provided by a company called Quarterdeck and we bought all the

rights to it and turned it into CME-Co Remote as a product offering and for internal use".

Knowledge is **captured** or retrieved from the numerous reservoirs distributed throughout the organisation. As described by the IT Manager "experts are just a phone call away if we have an issue or fault with one of our thousand or so of critical systems". "Each group within the ISS function has specific roles and responsibilities creating an extensive pool of experts", as stated by the [Cork] Security Officer. Each member documents or acquires solutions and best practices and makes them available throughout the function. Members of the ISS function generally have "access to everything except to some HR systems", as stated by the [U.S.] Security Coordinator. Knowledge is difficult to retrieve from MS Outlook as it can be "difficult to find solutions afterwards", as explained by the [Cork] Security Officer. As explained by the Corporate Security Officer, "everyone makes their fixes available through the different repositories or websites so that we can help one another out – obviously product designs are restricted but everything else is generally available". He further explained that "we use platforms like E-Room and Power-Link to work with our vendors [partners], competitors and customers".

Knowledge is continuously **created** through the problem-solving process used within ISS. Calls or problems regarding IT or IS Security systems are logged and assigned to members of the function. As explained by the IT Manager, "we solve issues or problems for the different business functions". The Portfolio Project Management Group (PPMG) was established specifically to ensure that each unit is supported by the function. As described by the IT Manager, "the portfolio mechanism used by PPMG is to facilitate the needs of our units when approved by Finance". He further explained that, "nothing can get done in IT without having approval". M-Gates is the project methodology used to manage the different project phases. As stated by the IT Manager, "specifically projects move from different phases, to get from phase one to phase two you actually have to pass a gate and there is a specific set of requirements needed to get past the gate". According to the [Cork] Security Officer, "you get a request in from a business function and we have to prepare what we call a value statement which is a single page showing the business problem and the impact that the business problem is having on the business, the vision in terms of what we want to do to resolve it and we need to quantify some benefits". As stated by the IT Manager, "the goal is to focus everybody on what we are doing is meeting some business needs. A project needs a level of approval – to do so you [for Customer Support] create a value statement, we [ISS] review it with the particular business unit and then it is listed on an approved projects list". As described by the [Cork] Security Officer "a member of the group is [then] identified as the lead for an initiative and that person knows what's happening and would coordinate with a developer or the respective portfolio person who will identify this as big enough to be a project or is it small enough to be what we call a continuous improvement (CI) initiative". As explained by the [U.S.] Security Officer, "if someone is approved to work on a project they will have access to all information unless it's very confidential financial information or HR information, generally speaking people will have access to business requirement documents as we go through the phases and gates, things like business requirement documents, functional designs all those documents are prepared as you go through that process and they are available to everybody [working] on the project".

One of the global projects "initiated across the multinational and implemented by the ISS function is Sarbanes-and-Oxley and we have implemented a whole series of procedures to support SOX requirements in the U.S.", according to the OISRM Coordinator. As stated by the Corporate Security Officer, "one of the requirements of SOX is that the executives of a company have to be able to certify all of their business requirements, all of their financial results, our auditors have to be able to certify them and when they take it down one level deeper that says that systems and transactions on the systems have got to be auditable which means that every change made to a system has to be auditable". He further explained that "any change that is made to a production system that could have an impact on our financial statements has to be documented, approved and segregation of responsibilities has to be implemented". As explained by the [U.S.] Security Coordinator, "segregation of responsibilities is enforced when the person who writes the requirement has got to be different to the person who writes the code, who has to be different to the person who puts that code into production and all those people have got to be different to the business user who requested it, so you got a lot of different people in there so that no one person can say hang on a second I am going to add a dollar to every transaction and feed it into my own bank account". It is used to enforce "checks and balances into the process and allocate responsibility to each step of the process and the decision-making involved", as stated by the IT Manager. Mechanisms such as "teleconferencing are used to coordinate any problems associated with SOX", as stated by the Corporate Security Officer. As described by the Corporate Security Officer, "we have these brainstorming sessions regularly to prepare for the many reviews by the internal audit committee and then the more important real audit".

As described by the IT Manager, "we improve after each audit, it's regarded now as an evaluation of all of the work that the different IT and Security groups do. Before SOX we were taken for granted unless something happened [a breach] we are now an important part of the process". The "OISRM was created to coordinate the entire organisation and ensure its correct implementation", as stated by the Corporate Security Officer. "My group was established to gain a competitive advantage from the compliance issue and identify our customer's requirements, essentially providing them with a full package with our storage offerings", as stated by the Corporate Security Officer. OISRM sources standards and best practices externally and "customises them internally by using the internal pool of experts and the audits feedback reports", as stated by the [U.S.] Security Coordinator. This type of collaboration is facilitated through "conference calls and discussion forums [E-Room]", as stated by the [Cork] Security Officer.

An audit is a learning process achieved through "trial and error – we work closely with J.P Morgan during their survey process and determine what worked and didn't, there is also a time to improve on any weaknesses and generally our work improves after each review", as stated by the Corporate Security Officer. As explained by the [Cork] Security Officer, "we take time after each review to set up a teleconference with all of the Security Officers and OISRM and work through the review and document the lessons-learned by the group". He further explained that, "the lessons-learned is the 'to do list' for the next audit [usually created by the internal committee] which are documented properly and stored in our shared drives as well as on our internal websites". As explained by the Corporate Security Officer, "auditing is a never ending process that we hope improves each time we are reviewed, it certainly makes us [groups] work closely so that the review goes well". He further explained that guides

such as the "ISO17799 and our security policies are always evolving to incorporate new environmental changes", and as a result aid in decision-making.

The ISS function **shares** knowledge through its problem-solving processes. As explained by the IT Manager, "everyone has to share knowledge, like solutions to solve the many issues that we face". The portfolio mechanism "is the approach we use to collaborate outside of our group with the business units, each has a dedicated portfolio manager who coordinates the process from the creation of a business case, approval [by Finance] to the allocation of IT resources to build a database or to apply security controls". He further explained that "a dedicated IT portfolio manager insures our needs or IT itself would be neglected". As described by the [Cork] Security Officer, "we share solutions, best practices and online resources [website addresses] all the time especially when we are working on a global project like SOX or the marketing knowledge management initiative [the central repository]". "Email, E-Room, Primus and Channel CME-Co are the main places we store [security] knowledge", as stated by the [Australian] Security Officer. According to the Corporate Security Officer the organisation "uses E-Room to trade interoperability knowledge for our products with our partners and competitors as well as allow our customers to have access to [some of] our product fixes [patches]". He further stated that "we are active members of regulatory bodies so that we can work with other companies in agreeing on standards [and facilitating interoperability] and that's not because you want to work with your competitors it's because your customers tell you that you need to work together".

The process of knowledge **application** or use is extensive in the ISS function. As described by the OISRM Coordinator, "knowledge such as standards and steps to implementing best practices is always being applied in CME-Co, we have to or we would not be compliant". He further stated that "all of our problem-solving for initiatives like SOX or even the implementation of a database require us to use documented procedures which we always try to improve through our regular conference calls between the different groups or the onsite [subsidiary] Security Coordinators". As explained by the Corporate Security Officer "SOX forced the company to change and document everything [access rights, and internal processes] it gave IT and OISRM more control but at the same time took it away as Finance direct and approve the changes. It forced us [ISS function] to allocate processes and document them, document every change and re-examine them for every internal audit and external audit". According to the IT Manager "it [SOX] forced us to make changes to the way we manage IT and security, the audit became a security and IT process that is always changing. It cost us a lot of time in the beginning but it has become easier with each Audit".

Knowledge **control** is necessary to assure the validity and utility of knowledge. As explained by the IT Manager, "we allocate controls based on the value of the data or knowledge". He further stated that systems are prioritised "according to the loss of money if a critical system is down or loss of time to market if our Engineering databases have been accessed and designs stolen". "Time to market is very valuable to a company like ours – it's essentially the release of one of our products before a competitor" as stated by the Corporate Security Officer. He further explained that, "we have had instances when our products were reverse-engineered and released by one of our competitors so allocating the right controls to design databases is vital. Our Engineers are also aware that they can leave any time if they choose not to comply with our code of ethics and unknowingly share a design with a competitor". According to the

Briefing Centre Manager, “Engineers will not share with Marketing, Customer Support or Sales but they do talk to other Engineers at conferences for example”. As explained by the Corporate Security Officer “companies are concerned about what it means to protect their knowledge given that you have continued breaches of security and now you have potential legal fallout from those continued breaches and so companies including us are looking beyond firewalls, VPN, IDS and prevention”. As a result, companies are hiring compliance officers in order to try and understand that very complicated legal and compliance environment and try and rationalise it in a way that is meaningful and can continue to do business. “Technologies are deployed to comply with a regulation without thinking through the impact of the technology side of it. For example, technologies like encryption even though there are significant issues with regard to the use of encryption, regulations do not take that into account and so you have an increase in the use of encryption even though you can actually lose access to the data or knowledge”, as explained by the Security Officer. The Corporate Security Officer stated that, “the only way is to protect your source code, you limit access to the data to those only authorised or needed to use it. So when you have CME-Co, people working on certain projects are continually reminded of the need to keep confidential data confidential and so you have got code names for certain projects for the next version of a product for example and the Engineer working on things like that are continually reminded that employment is at will and we are all free to move on and get another job and at the same time if we are in breach of compliance as far as the company’s policies that there are controls and procedures that you need to comply with as far as protecting that is concerned and you can’t lock down security in such a way that you couldn’t even theoretically, possibly have a breach or leak of source code”.

The IS Security KM processes identified within the organisation are summarised in Table 5.9.

IS SECURITY FUNCTIONS: KM PROCESSES	
Processes	
Acquisition	• Documentum – to utilise collaborate SW-E-Room for joint projects with Partners • Regulation Guidelines – bought and customised to comply with environmental laws • Interoperability Knowledge – collaborative initiatives for (Security) product development • External Consultants – Auditors for reviews of controls and network testing • Reverse-engineered – Security technologies purchased and customised for use and sale • ISO17799 Guideline – Purchased and customised • Subscription to Technical Groups – Manuals, Recovery Procedures, Updates and Tools • Online Tutorials – Purchased customised and delivered through Knowledge-Link • Security Specialists – Hired for specific projects
Capture	• CME-Co Reservoirs of Knowledge (Table 5.5) • Pool of Experts /Roles and responsibilities • MS Outlook/E-Room/Power-Link
Creation	• Problem-solving Process – in creating a solution • PPMG Mechanism – to create a business case • M-Gates – Project Management Method for a divide and conquer approach • Auditing process – Checks and balances / Trial and Error Learning Process • OISRM Group – Goal to retrieve, customise and share ISS practices and procedures • Brain storming – for documenting lessons-learned • Conference Calls/Discussion Forums • Lessons-learned – documented for the next project
Sharing	• Problem-solving – Sharing knowledge to solve and problem or fix • PPMG Mechanism – Collaborating through groups • Coordination - through Portfolio Manager • Email, E-Room, Primus, Channel CME-Co • Knowledge Trading – between members. • Active participation – in regulatory bodies
Application	• Reuse of customised standards, practices, solutions and fixes • Auditing – forces documentation and lessons-learned • Pool of Experts – use develops through trading
Control	• Allocation of the following controls: • Informal controls such as policies regarding behaviour • Formal controls regarding compliance • Technical controls such as VPN, IDS

Table 5.9: IS Security KM Processes.

The preceding sections depict the IS Security and Customer Support functions operating within CME-Co. The different types of knowledge used by the functions are described, reservoirs of knowledge pinpointed and the processes used to manage knowledge by the functions illustrated, and summarised in Tables 5.1 to 5.9. The next section compares the approaches used by the two functions to manage ISS and CS knowledge.

5.1.5 IS Security and CS Functions Managing Knowledge

This section considers CME-Co's IS Security and Customer Support functions approaches to managing their knowledge. It extends the descriptions discussed in the preceding sections by comparing the approaches used. The different types (Table 5.10), locations (Appendix D), and knowledge processes (Appendix E) are compared and then contrasted. Next, the mechanisms used to promote the management of ISS and CS knowledge are described in section 5.1.6. These are categorised as technological and non-technological. Use of the different KM tools is outlined and illustrated to determine individual and function usage (Table 5.11). Finally section 5.1.7 concludes with a description and discussion of the impact gained due to the management of knowledge on the (ISS or CS) individual, functions (products, services and processes) and the organisation (Table 5.12). Furthermore, display matrices are utilised to illustrate functional characteristics, differences and outcomes for each of the variables described. Each display matrice was reviewed and verified by the Security Coordinator and Knowledge Consultant (Table 5.2).

5.1.5.1 Types of Functional Knowledge

This sub-section summarises the different types of knowledge utilised by the CME-Co's IS Security and Customer Support functions. Table 5.10 is adapted from Tables 5.4 and 5.7. Table 5.10 summarises the different types and roles of knowledge used by the two functions to illustrate the similarities and differences. IS Security (Sec) and Customer Support (CS) knowledge (K) is categorised as general, technical and contextually specific knowledge. These are then further subcategorised as declarative (explicit/tacit) or procedural (explicit/tacit). The roles of each are identified, in Table 5.10, as operational (O), tactical (T) and strategic (S). Role totals are calculated from Tables 5.4 and 5.7 and used to compare the importance of each type of knowledge to each function (for example general operational knowledge has a ratio of Sec K= 11: CS K=12).

General knowledge is used for day-to-day operations within the functions. The IS Security function regards the following as general knowledge: hardware (HW) and software (SW) specifications, regulations, threats, email warnings, procedures and escalation levels as operational knowledge. The interviewees did not identify their general knowledge as tactical or strategic but "for everyday use and pretty much basic for our role", according to the [Cork] Security Officer. Customer Support also identified email warnings of possible errors, regulations and escalation levels as operational (Sec K=11: CS K: 12). However the "priority of hot issues" and the "approach used to solve a problem" were categorised as tactical by the function (Sec K= 0: CS K= 2). Hot issues, pertaining to the company's product portfolio, are tactical as they can, if prioritised, provide tangible benefits to the CS function. Prioritising hot issues can "reduce the workload of [Level 1 and 2] Technicians by eliminating the knock-on effect of one product failing, and it can also reduce our customer response time", as stated by the CS Manager. Problem-solving is the goal of the Customer Support function so the approach used to solve a problem is "always reviewed so that we can improve the process – the customer always comes first and the better and faster we are the more loyal our customers are", as explained by the KMS Engineering Trainer. Therefore CS general knowledge is regarded as tactical due to its impact on productivity. Time is saved as Technicians can prioritise and reuse solutions. The importance of the

knowledge expert is also emphasised as tactical knowledge is categorised as declarative and procedural tacit knowledge.

Technical knowledge is specific to either function. Lists of errors and documentation are regarded as technically operational by the two functions. Customer Support identified twice as many types of technical knowledge as operational (Sec K=4: CS K= 10). This is due to the fact that solutions, once created, are stored and shared but the process is very much a day-to-day activity. The product portfolio is also wide and complex requiring constant support, making solutions to customer problems dated as they are generally fixed before new (product) updates are released. Regulations, product specifications, lists of stored solutions, errors, and knowledge of customer environments are "fundamental to the objective of the [Customer Support] function", as stated by the KMS Engineering Trainer. IS Security primarily views technical knowledge as tactical. The allocation of access control lists to enforce the segregation of duties is "an everyday job but it is necessary and important in protecting the data and knowledge in the organisation", as stated by the [Cork] Security Officer. Tactical security knowledge is used to implement regulatory constraints and in identifying risks to CME-Co systems. Knowledge regarding regulations and standards are viewed as tactical as compliance is an environmental issue for the organisation. Customer support also views regulatory knowledge as tactical, as working with customer products can have regulatory implications, particularly if the problem is due to interoperability issues and the customer is located in another country. Additionally, the CS function views its ability to diagnose interoperability problems and errors as tactical. "Diagnosing errors is an invaluable tool as it requires [the] skills of our experts to trace an error that could be buried in lines of code or an interoperability problem with one of our customers systems – either way it's a skill that we can't teach; it's learnt through experience", as stated by the KMS Engineering Trainer.

CS therefore views its approach and ability to diagnose problems as tactical in solving calls and Security views the implementation of regulatory procedures as tactical, as non adherence could result in financial penalties for the organisation (Sec K=6: CS K= 4). However, IS Security has identified security: policies, regulations and strategies as strategic while CS does not view its technical knowledge as such (Sec K=5: CS K=0). This can be attributed to the role of the Global IS Security function. The security policy must be aligned to the strategy of the organisation so that it can support it and manage known security threats. Regulatory knowledge is imperative to the function as it has a dual role of protecting the organisation from internal risks and the risks associated with non-compliance (removal from the stock exchange).

Contextually specific knowledge is viewed as tactical by IS Security, with audit reports and procedures as its main resource. CS identifies its solutions and ability to solve problems as tactical (Sec K=9: CS K=3) but primarily this knowledge is viewed by CS as operational (Sec K=5: CS K=11) due to the role of the function, which is to "fire fight problems that are identified by our customers", as stated by the CS Manager. "Problem-solving is a core activity for Customer Support and the faster the solve, the cheaper the activity", as explained by the KMS Engineering Trainer. Templates, product errors, solutions (which are quickly dated), bugs, lessons-learned and the steps to diagnosing a problem are operational as these are "basic [knowledge] for our Customer Support organisation [function]", as stated by the Knowledge Consultant. However the ability to reverse-engineer, while a threat from our competitors is also regarded as a

tactical ability by CME-Co. As explained by the Operations Manager, "they [technological companies] all reverse-engineer [in order] to be the first to market and to figure out customer problems, as half of the time it's an interoperability issue and our Engineers have to reverse-engineer a competitor's product to diagnose a customer's problem. CME-Co doesn't wait for the fault to be allocated to the right vendor; we fix it because we know the customer will appreciate it and view us as the go-to service provider and not our competitors".

The totals illustrated in Table 5.10 indicate that CS knowledge is viewed by the CS function as primarily operational (Sec K=20: CS K= 33), and IS Security as tactical (Sec K=15: CS K=9). It is surprising that the CS function does not view its knowledge as strategic to the company but predominantly operational. Customer or product problem-solving is the function's core purpose (CS K= 33 O| 9 T| 0 S). While the activity is knowledge-intensive and utilises a KM initiative the function is not promoted or supported at a senior level but regarded structurally as an operational function. KM roles were established on an ad hoc basis and the initiative itself is driven purely at the CS level, by Knowledge the Champions. The KCS is regarded as a community of practice (CoP) consisting of CS Engineers evaluating the quality of solutions created, stored and shared within CS. The omission of KM from the organisational structure reduces the strategic and tactical significance of CS knowledge within the function.

It is evident that IS Security knowledge is regarded as strategic particularly vis-à-vis the company's security policy and strategy (Sec K= 20 O| 15 T| 5 S). The importance of IS Security knowledge can be attributed to the structure of the corporation as well and the business environment it is operating in. IS Security is a futile function if it is absent from the organisational structure. CME-Co has also identified compliance as a customer requirement and as a result formed a Corporate Security group to target customer regulatory requirements and generate additional income. The organisation has also created a group (OISRM) to source and customise regulatory standards and best practices in order to adhere to regulatory needs. Compliance has forced managerial responsibility in aligning security to the corporate strategy. It is through the IS Security function that controls (formal, informal and technical) are allocated to systems and employees in meeting regulatory requirements. The steps in applying standards for regulatory requirements are vital to the function. Security experts (Officers and Coordinators) utilise regulatory and control knowledge to ensure compliance and follow external advice regarding audits. The importance of the function is represented in the reporting structure of the organisation. The function reports to the Chief Information Officer (CIO) who in turn reports to the Chief Financial Officer (CFO), emphasising the financial implications of the function and therefore the strategic importance of ISS knowledge and the necessity to map ISS to every business function, and process.

Table 5.10 summarises and compares the functional view of IS Security and CS Knowledge utilised.

ISS AND CS FUNCTIONAL KNOWLEDGE												
D:E/T |P:E/T		IS SECURITY KNOWLEDGE	ROLE				CUSTOMER SUPPORT KNOWLEDGE	ROLE				
General Knowledge	D:E	Org. Doc.| Vendor |Internal Warnings| Threats	O			D:E	Org.Doc| Email Warnings| Customer & Engineering Errors	O				
	D:E	HW/SW Specifications: Firewalls/Servers	O			D:T	Regulations| Escalations| In/External Roles	O				
	D:T	Regulations| Impact of Threats| Roles| Escalations	O			D:T	Priority of Hot Issues & Errors	T				
	P:E	Procedures| White Papers – Projects ISS Issues	O			P:E	Emails: Bugs| Steps	O				
	P:T	Steps to Align IT & Access Control Lists (ACL)	O			P:T	Problem-solving Approach | Logged Call	T				
			O	**T**	**S**			**O**	**T**	**S**		
		Totals:	11	0	0		**Totals:**	12	2	0		
Technically Specific	D:E	IS Security Policy| Strategy| Regulations	S			D:E	Doc. of Regulations| Products| Environment	O				
	D:E	ACL & Alert Reports from Security Technologies	O			D:T	Regulations| Diagnosing| Interoperability| Bugs	T				
	D:T	Domain Access Rights: Segregation of Duties	O			D:T	Existing Solutions	O				
	D:T	Implement Regulations| Systems| Risk Knowledge	T			D:E	List of Errors & Solutions|	O				
	D:T	Advising Customers: ISS Issues & Tools	S			D:T	Diagnosing & Solving a Problem	T				
	P:E	Standards & Procedures	T									
	P:T	Developing Plan & Strategy| Security Methods	S									
			O	**T**	**S**			**O**	**T**	**S**		
		Totals:	4	6	5		**Totals:**	10	4	0		
Contextually Specific	D:E	SOX Requirements| Risk Criteria| Manuals	O			D:E	Solutions| Template| Product Errors	O				
	D:E	Audit Reports: Evaluation Feedback| NW Testing	T			D:E	Product Solution.	T				
	D:T	ISS Specialists Knowledge of: SOX| Risks| Audits	T			D:T	Bugs| Diagnosing| Lessons-learned	O				
	P:E	ISS Teams: Steps for Standards| Review	T			P:E	Solutions| Steps| Diagnosing	O				
	P:T	ISS Officers: Steps for: Incidents| Audits	T			P:T	Customer Feedback| Reverse-engineering	T				
			O	**T**	**S**			**O**	**T**	**S**		
		Totals:	5	9	0		**Totals:**	11	3	0		
		ISS Knowledge Totals:	**20**	**15**	**5**		**CS Knowledge Totals:**	**33**	**9**	**0**		

***Declarative (D)/ Procedural (P), Explicit (E)/ Tacit (T). \| *Roles: Operational (O), Tactical (T) Strategic (S).**
***Totals are calculated from Tables: 5.4 and 5.7.**

Table 5.10: CME-Co IS Security and Customer Support Knowledge (Adapted from Tables: 5.4 and 5.7).

5.1.5.2 Functional Knowledge Reservoirs

This sub-section describes the different reservoirs of knowledge utilised by the Case's IS Security and Customer Support functions. Appendix D is adapted from Table 5.5 and Table 5.8. The Table summarises the similarities, and differences between the IS Security and Customer Support reservoirs. The third column is derived from identifying the different reservoir characteristics from the two functions. The knowledge reservoirs of the functions are categorised by their practitioners, functions, artefacts and inter-organisational relationships. These different stores or reservoirs of knowledge are discussed in the following sub-sections.

(1) The knowledge residing in **individual members** or practitioners of a function can be identified through the roles and responsibilities attributed to them. Problem-solving specialists are used by the functions to diagnose a customer's problem or prepare for an audit. Engineers are used to design and build the products supported by CS and secured by ISS.

IS Security Engineers utilise the requirements identified by the Corporate Security Officer (Stakeholder Analyst) to incorporate security add-ons to existing and new products. Specific roles in IS Security have been officially created to target and identify market demand for security enhancements and aid customers in meeting their own, for example, regulatory requirements. A Director of GIS is responsible for sourcing appropriate standards, best practices and formulating corporate guidelines for CME-Co. This senior role provides the ISS function with political power in the organisation. Each subsidiary or site has an allocated Security Officer to coordinate and implement corporate guidelines and ISS controls. Security Officers or coordinators report to the site IT Manager and directly to GIS.

The CS function is managed directly by a CS manager. The manager is responsible for coordinating the different levels of support and developing support procedures. A Knowledge Consultant was identified by the CS function to tackle the enormous challenge of centralising knowledge for CS. This role and that of the Knowledge Champion is ad hoc and specific to CS. However a KDG (Knowledge Development Group) Officer was appointed in each CS site to identify the training needs of the different support levels. KCS writers are also used to review the quality of the solutions created by the function across the CS organisation. KCS writers have dual roles. They are quality reviewers but primarily CS Engineers.

It is from the above descriptions of the different roles and responsibilities within the two functions that the following characteristics were identified: problem-solving expertise, KM leadership/championship to promote KM, stakeholder analysis, senior roles sourcing/ assessing best practices and providing ISS with political support across the organisation, skills development coordination and external evaluation to assess core activities. Each of these roles provides invaluable expertise in the external and internal operations of the two functions. Additionally while ISS is promoted across the organisation, CS is internally focussed (Appendix D: Row 1).

(2) The group or function reservoir of knowledge is an extension of the practitioner store. The practitioners identified are a part of an internal function or an external source of expertise. Managers in the two **functions** are responsible for identifying policies, standards and procedures. Security Officers and CS Engineers are used to coordinate the different subsidiaries in order to support operations. ISS and CS use customer feedback (collected by Sales in product evaluation and the Corporate Security Group in identifying stakeholder requirements) as a guide or measure productivity and as a source of market demand.

ISS utilises a two-pronged approach to securing CME-Co. Two groups were established as separate (yet interacting) entities in order to specialise in specific aspects of security. The OISRM acquires and customises regulatory knowledge for dissemination throughout the multinational and provides a pool of expertise in compliance for audit committees and Security Officers to utilise. The Corporate Security Group is used to ascertain the security requirements of customers and incorporate security (for compliance) enhancements as a competitive advantage for the firm. Internal audit committees are used to evaluate internal processes and access rights in preparation for an actual audit. A Remote Services Group assesses and provides a secure communication link to external partners and customers. The CS function utilises an escalation process to effectively utilise the tacit knowledge within CS and Engineering. The higher the level of support required the higher the cost for CME-Co. To increase the skill-sets within the function a Knowledge Development Group was formed to enhance lower-level CS support skill-sets and ultimately reduce costs. Additionally, CS established a solution quality team to review and evaluate new solutions to improve the quality of support provided to customers.

It is from the above descriptions of the different groups interacting with the two functions that the following were identified: managerial collaboration, compliance adherence, innovative and creative teams, skill-set development group, domain (function) specific knowledge, measuring or evaluating external group, controlled external communication, and internal quality review committees. Each function utilises other functions or groups to evaluate activities. Even customer feedback is collected by Sales. CS primarily uses internal quality assessments. ISS established a group to regularly and formally collect stakeholder requirements and employs an external evaluator to measure ISS activities to ensure compliance but to also improve processes through post-mortem evaluations (Appendix D: Row 2).

(3) Knowledge is stored in practices, organisational rules, routines and **procedures**. The IS Security function utilises numerous procedures to ensure its compliance to different regulations. Procedures, standards, checklists and best practices are purchased from standard making bodies and customised to suit the needs of CME-Co. The procedures contain steps and guides for assuring the security of the multinational. They are customised to suit the needs of the organisation and the environment in which the organisation operates. A project management methodology (M-Gates) is used by the function to generate outputs at different stages of the project life cycle. This allows the function to collaborate with other functions and set deliverables. The function also uses a resource allocation justification procedure, Six Sigma, to essentially build business cases for

internal projects when competing with other functions for resources. However, Customer Support uses a limited number of procedures. A template is used to structure the solutions to customer problems and enable effective searches and consistency through the application of a template standard. The limited number of procedures is due to the closed environment in which the CS function operates. IS Security is a cross-organisational support function which must ensure CME-Co's adherence to policies and regulations.

It is from the above description of the different procedures used by the two functions that the following were identified: compliance or regulatory guidelines, standardised templates, to-do lists (check lists), documented (escalation) levels of expertise, business case requirements and a project management methodology (Appendix D: Row 3).

(4) Knowledge **repositories** can be paper-based (manuals, White Papers), or computer-based. The two functions primarily use the same repositories. A documentation management system (DMS) is used for ISS and CS solutions or fixes, the Intranet for corporate information, presentations, and group websites. The two functions make use of vendor specific repositories for product installation guides or specifications. E-learning resources such as Knowledge-Link are used for online training courses and portals to collaborate with partners and customers. However, the IS Security function identified their desktops and shared drives as personal and group repositories. Technical repositories subscriptions are used as a source of patch updates and procedures, and Q&A repositories for ISS queries. Customer Support uses a discussion forum for managers to collaborate in formulating common procedures and goals. The CS function is also dependent on notifications from Engineering regarding "hot issues", or priority errors and solutions.

Customer Support regularly tries to gain access to the Engineering Bug Tracking Systems to retrieve known errors/bugs and solutions. CS can spend hours and even days trying to solve an error that could already exist in Engineering's Bug Tracking Systems. This issue was raised repeatedly by CS interviewees as a considerable waste of resources. Engineering interviewees regarded the partitioning of the repositories as a fundamental approach to controlling their knowledge (product designs) and ensuring that any (known) risks which could seriously damage CME-Co's reputation are monitored (dangerous commands used incorrectly in a customer's environment). However it is important to note that access to functional and group systems is domain specific. That is once you are a part of a function you have access to the functions resources (unless denied by the authoring/designing Engineer). Engineering have complete control over their systems, labs and therefore networks.

It is from the above descriptions of the different repositories used by the two functions that the following were identified: documentation management systems (DMS), solutions, external sources of technical expertise through vendor repositories, shared platforms such as: drives, forums, Extranet, Intranet, portals, function websites, collaborative E-learning systems, email warnings and hyper-linked or integrated solutions (Appendix D: Row 4).

(5) Knowledge is stored in firm-specific **technologies**. The two functions use technologies to store and retrieve function specific knowledge for day-to-day operations and other activities such as auditing. Primus, the CBR tool, is available to the two functions. The tool is primarily used by Customer Support. Additionally the two functions over-use the corporate email system as a problem-solving platform to collaborate in creating and sharing solutions. The reported disadvantage to the utilisation of email is the difficulty in managing and retrieving solutions, documentation after a period of time.

Securing and monitoring a geographically dispersed environment is extremely difficult. ISS does, as a result, utilise a number of security technologies to aid in monitoring and protecting the multinationals corporate boundaries from internal and external risks. VPNs are used to encrypt external and internal lines of communication, SID for access-control and reporting, monitoring tools to generate alert logs, firewalls for enforcing internal/external access rules and IDS to track internal and external network traffic. Each technology generates streams of data which is pulled into monitoring databases in order to filter, query and generate a view of the CME-Co's security landscape.

It is from the above descriptions of the different technologies used by the two functions, that the following were identified: problem-based reasoning tools, monitoring and tracking technologies and combined integrated analysis through ISS technologies (Appendix D: Row 5).

(6) Knowledge is also stored within entities such as other **functions**. The ISS function interacts with every other function within CME-Co. It is through, for example, collaborative projects that security requirements are identified and (resource permitting) allocated. CME-Co utilises a Portfolio Project Management Group (PPMG) to identify function requirements and facilitate collaboration between the different business and technical units. It is also one of IS Security's tasks to know and understand functional roles and responsibilities in order to enforce segregation of duties across CME-Co under the governance of the Finance and Legal departments.

However, the CS function interacts with a limited number of units. It interacts with Engineering, R&D teams, ISS, IT and Sales. Internally CS is referred to as a customer supporting organisation operating within CME-Co, sitting between Engineering and the corporate customer-base. This is due to its core role of supporting the CME-Co product portfolio and fire-fighting problems.

It is from the above descriptions of the different units/functions interacting with the two functions that the following were identified: cross-functional collaborative projects, project management mechanism, segregation of duties and governance (Appendix D: Row 6).

(7) Knowledge is also stored in **inter-organisational relationships** or **networks** such as collaborative partnerships. The two functions make use of inter-organisational relationships in order to collaborate on specific projects. Vendors are used to provide product and technology specifications. CS requires access to the product specifications of their competitors so that they can resolve a

customer's interoperability errors. CME-Co customers can use several products from many different vendors in their environments. Additionally the CS function uses customer feedback as an informal review mechanism.

ISS also use external knowledge sources. However ISS does employ a Corporate Security group to determine stakeholder (customers, partners) security requirements. This group is used to increase the organisation's competitive advantage by identifying how security (services and tools) could generate additional income. The ISS function also participates in and drives regulatory bodies to guide the ISS and storage market/s and therefore create business opportunities. External auditors are used as evaluators for regulatory purposes. Audit reports are also used as a form of measurement to determine the usefulness of the function to CME-Co. Finally the two functions use Power-Link and E-Room as internal and external collaborative platforms.

It is from the above descriptions of the different inter-organisational relationships or networks that the following were identified: stakeholder feedback, Extranet, partner collaborative software, industrial groups and external evaluation reviewers (Appendix D: Row 7).

In summary, the different levels of expertise are viewed as a significant source of knowledge within the two functions. CS created an ad hoc Knowledge Development Group (KDG) and Coordinator to develop lower level support skill-sets and ensure solution standards through a quality review mechanism or group (KCS). Procedures such as solution templates and management techniques are viewed as important sources of knowledge. Documentation from internal and external sources was used to comply with functional or corporate requirements, particularly in documenting lessons-learned and case solutions. Knowledge tools such as a CBR tool, repositories and email were used to store knowledge. It is also evident that both functions were dependent on inter-relationships with an external evaluator for the IS Security function. However the CS functions knowledge stores are primarily internal to the function. CS knowledge was focussed on the organisation's product portfolio and similar (competitor) product offerings. Therefore internal sources of knowledge are vital. The ISS function was differentiated by its position structurally in CME-Co. It was a separate function from IT, and reports directly to the Finance department indicating its structural and financial importance to the organisation. Additionally this ensures that ISS has political support at senior levels particularly in relation to regulatory drivers and evaluations. Groups (OISRM and the Corporate Security Group) were also established to focus on regulatory issues and identify stakeholder requirements. As a result the ISS function was dependent on external sources of knowledge.

5.1.5.3 Functional Knowledge Processes

This sub-section summarises the different knowledge processes utilised by CME-Co's IS Security and Customer Support functions. Appendix E is adapted from Tables 5.6 and 5.9. Knowledge is pulled from the ISS and CS reservoirs outlined in Appendix D and used through the processes outlined in Appendix E. The Table summarises, compares and highlights the differences between the processes used within the two functions. The third column illustrates the characteristics of the practices used to manage ISS and CS knowledge.

(1.) Knowledge **acquisition** is the process by which knowledge is obtained and transformed into a representation that can be internalised by CME-Co. Table 5.1 outlines the organisations propensity to (budget permitting) purchase companies in order to acquire knowledge and simultaneously enhance its product portfolio. The acquisition of Documentum in 2003 provided CME-Co with a pool of expertise in the development of web-based environments and the use of a ready-made collaborative web-based room. E-Room was purchased as an internal and external (suppliers, partners and customers) collaborative environment. CME-Co also purchased the rights to a remote access product (rapid remote) from a company called Quarterdeck. CME-Co Engineers reverse-engineered the tool, enhanced its functionality and repackaged it as CME-Co Remote. These corporate acquisitions are used by the two functions to enable secure collaboration.

ISS and CS use acquisitioned software to collaborate. Subscription to external technical communities of practice (CoP) and vendor repositories is fundamental to acquiring external knowledge regarding, for example, new security technologies, manuals and best practices. Training courses are also purchased, customised and delivered through Knowledge-Link. However CS uses simulations of the support lab to train new Technicians in fire-fighting. Corporate and competitor products are used in developing reverse-engineering and diagnostic skill-sets. Competitor's products are also reverse-engineered to understand how a competing product works and interoperates with the CME-Co product portfolio. This practice provides knowledge for training, problem-solving, product enhancement and competitor analysis. Best practices, regulatory guidelines, and standards are purchased and customised, by ISS, to comply with U.S. and international regulatory laws. External auditors and security specialists are hired to avail of their testing and audit expertise. Membership of regulatory bodies allow the IS Security function to ascertain the steps taken by other companies in auditing and reviews. CME-Co, as a result, participates in driving the market to stay ahead of its competitors. CS is dependent on its internal pool of experts and therefore acquires a limited volume of external knowledge. ISS sources a larger volume of external knowledge regarding its business environment to identify risks, threats, and adhere to regulatory requirements. Procedures, security technologies and software are purchased, and customised. External experts are also hired to refine audit reviews and evaluate the function and security controls used.

It is from the above description that the following were identified: collaborative platforms, customised guidelines, reverse-engineering and diagnostic skill development,

subscription to CoPs, external repositories, measurements, customised training and expertise (Appendix E: Row 1).

(2.) ISS and CS **capture** or pull knowledge from the different CME-Co reservoirs (Appendix D). The two functions use their respective pools of expertise to address function queries and problem-solving. The different roles and responsibilities allocated to individuals facilitate the identification of experts located across the multinational. Applications, such as email and portals, enable the functions to pull knowledge from the different reservoirs to collaborate, create, share, and store, for example, technical and product debugging solutions. ISS uses external experts to conduct evaluations in preparation for audits to test the level of security within the organisation, through for example network vulnerability testing. CS, primarily, captures knowledge with the case-based reasoning tool (CBR) Primus. The tool is used to capture, create, share, store and reuse solutions pertaining to the CME-Co product portfolio. The CBR tool facilitates external collaboration (Power-Link). Customers and partners can, once registered, retrieve existing solutions and create new solutions. Therefore CS can capture and reuse partner knowledge in solving CME-Co's product bugs.

The two functions capture external expertise. ISS uses evaluators to measure goals determined by the requirements of individual audits (particularly the previous audit). This is an ongoing review process requiring the documentation and adoption of lessons-learned from one review to the next. CS, in comparison, captures partner and customer knowledge to create solutions and then share the solutions internally and externally with other partners. CS has also identified the value in pushing knowledge towards partners and customers. Self-service enables partners and customers to solve their own problems and therefore reduce CS costs while simultaneously increasing CS productivity.

It is from the above description that the following were identified: case-based reasoning tools, pools of expertise, roles and responsibilities and collaborative platforms (Appendix E: Row 2).

(3.) The two functions **create** solutions through problem-solving. Lessons-learned are documented due to the utilisation of the M-Gates project management methodology and ISS audits. ISS creates and acquires evaluation reports (audit reviews), identifies security controls, customises standards and best practices for compliance deliverables. Mechanisms such as brainstorming (enabled through online forums and teleconferences) are used to conduct post-mortems of activities such as audits. CS creates solutions internally using the different levels of support (escalation process). Partners are also used to generate solutions which are shared through the online view of Primus (Power-Link).

The primary difference between the two functions in creating knowledge is that ISS use of an external evaluator. Mechanisms are widely used by the ISS function to facilitate the creation of new security knowledge and support other functions. The Portfolio Project Management Group (PPMG) identifies the security requirements of other business functions as well as those of ISS. Brainstorming, M-Gates and a coordinating security group (OISRM) are used to ensure collaboration in achieving ISS and corporate goals. However, the

evaluation and resulting documentation of audit reviews and lessons-learned is environmentally driven. CS identified the potential of leveraging the knowledge of CME-Co partners and vendors in creating and sharing new solutions (knowledge) to reduce costs.

It is from the above description that the following were identified: problem-solving process, business requirements mechanisms, project management methodologies, escalated support, and specialist groups for external collaboration (Appendix E: Row 3).

(4.) Knowledge **sharing** is the process through which explicit and tacit knowledge is communicated between individuals, functions or organisations. The ISS and CS functions share knowledge through the utilisation of tools such as email, E-Room, Primus, and Channel CME-Co. Problem-solving and levelled support (through the escalation process) also enable the generation and sharing of knowledge. Knowledge trading is also used. Help, in the form of an expert or a manual, is requested by one expert from another to solve a problem. The help is often traded to ensure collaboration at a later date or access to a knowledge store. The two functions exploit external knowledge to create and share solutions. Regulatory bodies are used to participate in the creation and sharing of standards and partners are used for solution generation. However the use of mechanisms can vary. ISS employs a coordinator and the PPMG mechanism to encourage the collaboration and sharing of knowledge, while CS uses the CBR tool Primus.

It is from the above description that the following were identified: problem-solving, PPMG mechanism, coordinators, knowledge tools, knowledge trading and participation in industrial forums (Appendix E: Row 4).

(5.) Knowledge **application** is used to guide decisions and actions. The two functions create, use, customise and store knowledge in the form of solutions, standards, and best practices. Pools of ISS and CS experts are used to collaborate, share and therefore use and reuse knowledge in making problem-solving decisions. However CS uses the CBR tool to store and reuse solutions. ISS exploits the auditing process to apply and reuse knowledge from past reviews as benchmarks for forthcoming reviews.

It is from the above description of the different that the following were identified: reuse of customised practices and solutions, documentation of lessons-learned, benchmarking, and knowledge trading (Appendix E: Row 5).

(6.) Knowledge **control** secures valuable corporate or functional knowledge. ISS is responsible for protecting corporate assets. However CS, and particularly Engineering are regarded by senior management as innovators who require complete control over their systems and networks. Engineering apply controls, such as access rights, to their own systems resulting in weak points in the CME-Co network. ISS uses formal, informal and technical controls to control the behaviour of individuals and unauthorised users. Tools and mechanisms are used to monitor and track internal traffic to identify or scan any rogue behaviour. CS uses controls such as tracking, monitoring and domain-specific controls to assure the validity and utility of the solutions created and stored in Primus.

It is from the above description of the different examples of knowledge control that the following were identified: controls (informal, formal and technical), tracking internal and external traffic, quality mechanisms, access rights, managerial reviews and goal setting (Appendix E: Row 6).

In summary, a significant amount of knowledge is acquired externally. Collaborative software, regulatory guidelines, subscriptions, products and external evaluations are acquired by the functions to ensure that the organisation is compliant with its business environment and aware of any and all business opportunities such as market changes and competitor product advancements. Problem-solving is the principal approach used to create knowledge and applied through the reuse of the solutions created and stored. The ISS function does purchase significantly more external knowledge than CS. This is due to regulatory requirements such as the Sarbanes-and-Oxley Act of 2002 (section 2.4.4) which requires the application of segregation of duties and adherence to environmental standards. However this environmental driver enabled ISS to exploit the auditing process and use reviews as benchmarking aids in applying lessons-learned to internal and external ISS activities.

5.1.6 IS Security and Customer Support KM Mechanisms

This section describes the **mechanisms** used in CME-Co, either directly or indirectly, to promote the management of ISS and CS knowledge. Table 5.11 outlines the mechanisms which are divided by type, and illustrates which are common or unique to both functions and as a result available at an organisational level (√√). The first sub-section describes the mechanisms used at an organisational level, and the second at a functional level. Finally, this section concludes with an analysis of the mechanisms used.

(1) Organisational Level

The company is rich in legendary tales of business daring and a culture of doing "whatever it takes to create customers for life" [CME-Co Website]. Induction training for CS Technicians, Engineers and ISS practitioners is used to provide "new hires with knowledge of key products, key clients and company specific skills such as M-Gates and [ISS] policies", as stated by the Learning Officer. New inductees are also "made aware of the founders of the company through analogies and story-telling, as well as Engineering Gurus", according to the Knowledge Consultant. Specific training such as "compliance courses or lab simulations are used in addition to the usual induction sessions, through E-learning from the CME-Co university", as stated by the IT Manager.

"Learning on-the-job through mentoring or job shadowing is very useful in building up relationships and reducing the time needed to get up to speed, but it isn't formal even though every business function does it, it's sort of on an ad hoc basis", according to the Engineering Trainer. According to the IT Manager, "face-to-face meetings in a globally dispersed organisation are very useful; you need to establish some sort of relationship with your colleagues especially if you're managing them". Additionally "the PPMG is very useful for integrating the different business functions. For IT it's vital in ensuring that we and Security meet our customer's needs and that our own [IT and ISS] are also met", as further explained by the IT Manager. As explained by the Corporate Security

Officer, "brainstorming at the end of each [audit] review is very beneficial, even more so if Deloitte [the Auditor] are involved or immediately after their feedback. It makes the next review far easier". "Recording lessons-learned at the end of a project or review is necessary for us to improve for the next project or review. Even for a joint project it is very useful to note how a competitor operates", as stated by the Corporate Security Officer.

As described by the Purchasing Manager, "the most useful technologies in CME-Co are; teleconferences, email, which is a nightmare to manage after a while, the Intranet and Excel. Even though we are a storage company everyone downloads to Excel, it's just easier than trying to find what you need through all the different Oracle views. We download, filter what we need to do our jobs and generate reports; anything else I need I can access Channel CME-Co, our [central] document repository, and E-Room to work with my suppliers". The organisation has also created specific groups and forums in order to coordinate different initiatives and core functions. As explained by the CS Manager, "the management discussion forum is used at a functional level for collaborating across subsidiaries. It is used to select key best practices and guidelines for specific functions". Groups such as the OISRM and the Corporate Security group were established "to drive our internal and external security agenda in compliance and in selling our security expertise", as stated by the Corporate Security Officer. According to the KMS Engineering Trainer, "the Knowledge Development group [KDG] was created in CS to develop our Level 1 and 2 training needs and the KCS team were established to act as a [solution] quality review community of practice". Additionally the role of the Knowledge Consultant was created to champion KM and "drive the centralisation of our internal knowledge".

The next sub-section describes the KM mechanisms used primarily by the ISS and CS functions.

(2) IS Security and Customer Support Function Levels

The ISS function avails of "vendor resources or repositories of best practices, security forums, M-Gates for project management and many, many teleconferences", as stated by the [Cork] Security Officer. Pagers also notify practitioners if there are alerts from the firewalls or IDS monitoring tools; and daily emails are sent from the OISRM group with warnings and hyperlinks to solutions or procedures. As explained by the Security Coordinator, "[the] SETA [security, education, training and awareness] programmes are useful in informing new hires about the [different] threats to CME-Co and to be wary of man-in-the-middle attacks as well as the penalties for breaking [security] policies". As described by the Knowledge Consultant, "CS uses the same tools available to every other function; common and individual shares – but we would prefer if employees would use E-Room for storing [individual] documentation, Power-Link for our customers and partners. Email, vendor websites, Q & As [forums], external technical forums and Channel CME-Co are also used".

The Engineering Manager explained that "multiple mechanisms are used to create, share and use knowledge in the CS arm of the organisation. We have a mechanism called subject matter expert programme [which] involves sending our people to work with [U.S.] Engineering for up to six weeks, where they shadow an Engineer, working with him, by front-ending calls. On their return they continue to front-end the calls saving the

[U.S.] Engineers time especially at three o'clock in the morning [due to a five hour time difference]". As described by the KMS Engineering Trainer and the Engineering Manager "valuable trusted relationships were created as a result, especially when the Engineers recognised the benefits [time] of mentoring – [Cork] Engineers". The disadvantage of the programme was, according to the Engineering Manager, "the cost in getting our people from here [Cork] or Sydney to the U.S. to work with the Design Engineers on a regular basis". According to the Engineering Trainer "the escalation or problem-solving process is another mechanism to ensure the quality of the solutions stored in Primus [the CBR Tool]". "Primus is used by CS and ISS to track calls and the escalation process", as stated by the Remote Services Manager. Experts are used to review solutions and technical writers from the KCS team are also used to ensure that fixes are valuable and follow the tools [Primus] template. "Initially this [solution process] wasn't monitored and the fix standard was poor and difficult to search [untagged]", as stated by the KMS Engineering Trainer. Prior to the introduction of Primus in 1994, "CS identified a number of inefficiencies such as: (1) lack of technical content, (2) content was often written at the wrong level, (3) little or no procedural information, (4) manuals were often written with insufficiently detailed information, and (5) technical information wasn't always added", according to the KMS Engineering Trainer.

As described by the CS Manager, "we [have] moved away from email and other sources of information points to effectively change information from document-centric focus to workflow focus and try and capture new information in the workflow". The Knowledge Consultant explained that, "end-users [CS Engineers, Engineers, Field technicians and trainers] wanted all the information regarding products in one centralised location. They did not want the process of finding a fix or answer to be a separate process and [needed it to be] integrated into the workflow - the day-to-day routine followed to service customers. Rather than finding the fix for a problem and later going back and recording it for others to use, users wanted to capture the information as it is developed and make it available to everyone to improve the service of products and prevent problems from occurring". However the CS Manager and Knowledge Consultant contend that, "the Engineering bug tracking system is completely partitioned from CS". Power-Link the Corporate Extranet, then "connects customers to the Customer Support, training, product, and interoperability information [in Primus] that they may need at any time", according to the E-Services Manager. "Customers can personalise their view so that the Knowledge tool makes it easier to find information and resources on the products that they use", as stated by the KMS Engineering Trainer. Customers and CS members can also "use Channel CME-Co [Extranet and Intranet] to locate an expert on a [particular] product", as stated by the Knowledge Consultant.

The next sub-section compares KM mechanism usage by the ISS and CS functions.

(3) CME-Co KM Mechanisms

KM mechanisms are structural methods used to promote the exploitation of KM tools and are supported by the organisational infrastructure (section 5.1.2). Table 5.11 outlines and summarises the forty-one KM mechanisms used within CME-Co which were verified by the Knowledge Consultant, KMS Engineering Trainer and the Security Officer. The proportion of mechanism usage, within the two functions, was high with seventy-eight percent of the mechanisms, available used. Overall fifty percent of the

mechanisms identified were categorised as organisational (used by the two functions). Twenty-one percent of the organisational mechanisms were identified as non-technological and twenty-six percent as technological. On the-the-job training, ad hoc mentoring, training, face-to-face meetings, brainstorming sessions, analogies, stories of business daring, the documentation of lessons-learned was each exploited by the ISS and CS functions.

The contribution of IS and CS practitioners to CME-Co was reported to be easier when knowledge was made accessible through technology. The content stored was explicit, shared and modified if required. CME-Co combines its document management system with Channel CME-Co (the Intranet) to provide centralised knowledge. The other mechanisms used by the two functions were identified as: common shares, technological forums, an Extranet for external collaboration, excel, email, vendor repositories, an E-learning platform, electronic contact lists, internal repositories, lessons-learned databases, hyperlinks and two-way pagers. The mechanisms used to facilitate socialisation included: cooperative projects across the functions (PPMG), repositories of best practices and lessons-learned. Combination was facilitated by collaborating through documentation management systems (DMS), databases, problem-solving, escalation processes and web-based access to knowledge.

The integration of CS practitioner expertise was regarded as a strategic initiative. Primus was created to combine explicit and tacit knowledge of CS practitioners. The CBR tool (Primus) was used to acquire and manage CS knowledge and distribute it within CS and among partners. The tool was used to disseminate and reuse the solutions created which ultimately improved the effectiveness of CS decision-making. Knowledge capture was also facilitated by Customer Support's case-based reasoning (CBR) tool. Knowledge sharing was enabled through the use of repositories, lessons-learned systems, expertise locators through contact lists and the corporate Intranet – Channel CME-Co. Knowledge application systems such as the CBR tool and the hierarchical relationships outlined in the structure of the organisation enabled practitioners to create, store, share and use solutions. The ISS and CS functions were also categorised as support centres and as such were used to facilitate direction, policies and standards used to support and protect CME-Co. Thirty-nine percent of the CS mechanisms identified were categorised as non-technological with just twelve percent technological. This low percentage indicated a significant difference in its use of non-technological mechanisms such as employee shadowing, simulated training and rotation in order to share Engineering expertise and build relationships between the different levels of support. CS utilised ad hoc groups and roles to coordinate the development of skills, and the incorporation of a quality solution review group. A Knowledge Consultant role was also created to coordinate the centralisation of CS knowledge across the dispersed support groups and levels.

Thirty-nine percent of the ISS mechanisms identified were categorised as non-technological with an equal percentage as technological. The ISS function utilised non-technological mechanisms such as SETA to control employee behaviour regarding external risks and threats to CME-Co. Formal groupings were established to drive the different facets of ISS. The OISRM and Corporate Security groups were established to source regulatory standards, coordinate internal security and identify customer and therefore market requirements. Additionally membership of and participation in regulatory bodies and ISS forums enabled the organisation to steer the ISS regulatory

market. Security technologies were used to pull data from across the geographically displaced subsidiaries to develop a picture of the CME-Co security landscape. ISS knowledge was also captured through solution templates and stored in repositories where it could easily be retrieved by ISS practitioners.

Table 5.11 illustrates the high volume of KM mechanisms used in CME-Co. It is evident that ISS utilised formalised mechanisms and external measures compared to Customer Support's ad hoc mechanisms to drive KM within the function. The significant difference between the functions was the use of the CBR tool. CS positioned its KM initiative around Primus. Due to the dedication of CS practitioners the role of the tool was gradually increased as its value to CME-Co was continuously demonstrated. Additionally, Primus was used to provide CS solutions and as a self-service support environment for CME-Co customers and partners. CS utilised quality mechanisms for the solutions created, allowed knowledge filtering and advanced search criteria's and pushed CS knowledge towards CME-Co customers. Therefore ISS was externally driven to comply with specific goals and measures due to regulatory requirements and CS was driven to develop skills and utilise practitioner knowledge more efficiently. ISS utilised KM mechanisms to supports the function's goals of protecting the corporate assets, adhering to regulatory constraints and sourcing environmental opportunities for exploiting the regulatory market. However the utilisation of a CBR tool and lab simulations could enhance the ISS functions effectiveness in supporting the needs of the organisation.

IS SECURITY AND CUSTOMER SUPPORT KNOWLEDGE MECHANISMS				
Mechanisms:		**Use**	**ISS**	**CS**
Non Technological	Induction Training:	Specialised for CS Technicians & Engineers	√	√
	Analogies:	Founders & specific Engineers are promoted as heroes	√	√
	Learning on the Job:	New staff are introduced to role gradually	√	√
	SETA:	Security awareness training for general new hires	√	
	Lab simulations:	CS Tools & procedures are taught in a fake CS lab		√
	Mentoring:	On an ad hoc basis	√	√
	Rotation:	With Corporate Engineering group – subject to budget		√
	Job shadowing:	Learning by observation		√
	Teleconferences:	Regular meetings with Security Coordinator & team	√	
	Face-to-face meeting:	Onsite & arranged ISS team meetings	√	√
	Development Group:	(KDG) Coordinating skills development & solution quality		√
	Quality Review Group:	(KSC) Engineers assigned to review internal & partner solutions		√
	OISRM Group:	Coordinating the roll down of ISS policies & best practices	√	
	Compliance Group:	Enhancement of products with security features	√	
	External Evaluation:	Auditors (Review) & Security Vendors (Penetration Testing)	√	
	Expert Status:	Identified through Primus for solution with most hits /use		√
	CME-Co University:	E-learning – for e.g. Six Sigma / SOX / SW Engineering	√	√
	M-Gates Method:	Step by step project management for collaborating	√	
	Brain storming:	Internal Collaborative Forum to Record Lessons-learned	√	√
	Informal Contact list:	To ensure that hires have a basic contact list – re function	√	
	PPMG:	Project Portfolio Mgt Group for Unit Requirements	√	√
	Knowledge Consultant:	To drive CS effort in centralising knowledge		√
	Problem-solving:	Escalation process	√	√
KM Technologies	Primus:	Case based reasoning tool		√
	Common Shares:	Function share drives	√	√
	Global Tech Forums:	External Vendor Repository of Best practices	√	√
	E-Room:	External collaboration & internal share	√	√
	Excel:	Used to summarise data from ERP for day-to-day use	√	√
	CME-Co Channel:	Intranet /Central document repository	√	√
	Email:	Warnings re threats/ bugs	√	√
	Vendor Repositories:	Product specifications / Security alerts & guidelines	√	√
	Knowledge-Link:	General online training – on request	√	√
	Mgr Discussion Forum:	Used at function level for collaborating across subsidiaries		√
	Power-Link:	Extranet/Customer & Partner access		√
	Eng Bug tracking Sys:	Limited access to CS / used for Eng solution generation		√
	Contact Lists:	Online & personal Expert pools list	√	√
	Repositories:	Best practices & guides	√	√
	Lessons-learned DB:	For recording end of a project / review	√	√
	Security Forum:	Collaborative Corporate Forum	√	
	Scanning SW	Monitoring the NW		
	VPN:	Tunnelling to protect communication	√	
	Hyperlinks:	Daily email warnings with links to solutions & guides	√	√
	Wireless technology:	2-way pagers from Firewall etc alerts / Calls	√	
***Organisational Level (√√): √ ISS** and **√ CS** *** Specific to One Function: √**				

Table 5.11: IS Security and Customer Support KM Mechanisms.

5.1.7 Impact of Managing IS Security and Customer Support Knowledge

This section describes the impact of managing IS Security and CS knowledge within CEM-Co. The direct and indirect management of this knowledge has impacted the organisation at the following three levels: (1) individual; (2) functional and (3) finally at an organisational level.

Level (1) Individual Impact

The management of knowledge has impacted employees in the IS Security function through "attendance at security conferences, employee reviews as well as external reviews", as stated by the IT Manager. As explained by the Corporate Security Officer "it makes our jobs easier as new security technologies are complex and [knowledge] tools and best practices help us keep ahead of threats like hackers". Ultimately the audit process helps the group improve, as according to the [Cork] Security Officer, "audits were a pain but they have become so much easier and are a kind of evaluation of our role".

CS has measured the impact of the use of its CBR tool on members. As explained by the KMS Engineering Trainer, "training has been reduced from six to three months, managers use a report [from Primus] of the number of solutions created by employees and the number of hits [solution use] during employee reviews". Employees also regard the CBR as invaluable "in keeping ahead of product changes", as stated by Level 1 Technician. Access to a "greater number of solutions makes our jobs a lot easier and [it] is ultimately recognition of our role within CME-Co", as stated by the CS Manager. Greater use of the CBR coupled with greater access allows CS employees to "tackle more calls and frees senior staff for more complex issues", as stated by the Knowledge Consultant.

Level (2) Functional Impact

As described by the OISRM Coordinator, "the overall performance of the group isn't measured using conventional means". "Return on investment is not suitable in measuring the value of security; we are measured in terms of loss of productivity due to system downtime or the time to re-establish a network", as stated the GIS Director. The ISS function "does not measure how well we manage our security knowledge, we look at ways to improve our processes, speed up decision-making and time necessary to get new members up to speed", according to the IT Manager. "Members know where to find security knowledge and who the different experts are", as stated by the Corporate Security Officer. "A [specialised] group was created to coordinate and share [best] practices and standards across the organisation", as stated by the Corporate Security Officer.

As explained by the CS Manager, "[increased] sharing across the different levels reduces cost and improves [the] productivity", of the function. Customer "problems are escalated through the different levels to develop new solutions", as stated by the KMS Engineering Trainer. "Someone in Hopkinton can easily use a solution constructed by someone in Sydney", as stated by the Engineering Manager. "The utilisation of Primus has made the support of a complex growing portfolio of products achievable", according to the CS Manager. "The benefits of our technological solution to our

knowledge management problem are numerous", as stated by the KMS Engineering Trainer. The use of the Primus solution allows "the collective knowledge of CS to be available to everyone for solving customer problems more quickly and effectively". The KMS Engineering Trainer stated that, "usage [internal and external combined] is doubling every eight weeks, freeing up Engineers".

(2.1) Product / Service Impact

As explained by the Security Coordinator, "best practices and standards are bought and evaluated to develop the best security solution for the organisation". "Diagnosing of problems increases [knowledge of Security groups and] response times for fixes", as stated by the IT Manager. Audits are used as "evaluations of our work but they are also used as an extra for our customers, we incorporate tools to make things easier for our customers", as stated by the Corporate Security Officer.

Capturing problems and questions from customers and "tracking the frequency of occurrence enables focused product improvements", as stated by the Knowledge Consultant. "If a solution is being continually reused, we can look at the root cause and fix it", as stated by the CS Manager. "Escalations and reverse-engineering are very useful in problem-solving", as stated by the CS Manager. Additionally if a solution is continually reused Engineering "can examine the root cause and fix new releases of the product", as explained by the Engineering Manager.

(2.2) Processes

As described by the [Cork] Security Officer, "brainstorming sessions at the end of a project allow us to record the results or lessons-learned, which will be useful for the next review or incident". A high number of external web sources; repositories, forums are used by Security Officers. "We know what's going on, more often than not – when we come in the morning we have emails warning us of potential threats and the steps we should take. The warning could come from the U.S. or McAfee", as stated by the Security Coordinator. "We do record [the frequency of] calls per customer and solves [per employee] internally but it's the reviews which are used by management to determine our value", as stated by the Security Coordinator. Compliance has forced the creation of "a security group as well as a stakeholder group to identify ways to sell security enhancements", as stated by the Corporate Security Officer.

CS uses "employee rotation to learn from Engineers, brainstorming sessions, use of forums, and the number of solution hits as measures for Primus", as stated by the Engineering Manager. Additionally "the longer it takes for a customer's problem to be solved, the more layers of support it travels through, increasing cost and utilising resources. Each successive layer is equipped to handle fewer and fewer calls. By pushing knowledge back toward the customer we are able to free up resources [money, personnel] which can be better utilised to improve products and get products to market", as stated by the Knowledge Consultant. The CS Manager further explained that, "every day spent by Engineers on customer problems is a day that the next generation of product will be delayed, thereby eroding our market advantage". Innovative solutions are pushed towards customers to reduce costs and time and therefore the use of internal stored and tacit knowledge.

Level (3) Organisational Impact

Security strategy is aligned to the business strategy "due to environmental drivers and the fact that poor security would have a dramatic effect on our image since we are a technological organisation and sell security", as stated by the Corporate Security Officer. As described by the GIS Director, "best practices are sourced and evaluated before we distribute them to the different subsidiaries. This enables us to be more effective in protecting CME-Co". As explained by the Compliance Officer, "the auditing process has made a huge difference internally and with our customers, we use compliance as a selling feature for our products and SOX gave the group a lot of [internal] political power". "Members are also learning how to apply their [security] knowledge effectively due to the evaluation process that we have now, through internal and external auditing", as stated by the Compliance Coordinator. Membership and coordination of "regulatory bodies allow CME-Co to drive and influence the market, it's the only way to stay ahead of everything and everyone", as explained by the Corporate Security Officer.

As described by the CS Manager, "it [Primus] enhances our relationship with customers". "The [KM] approach used here [CS] is just for CS [and not aligned to the business strategy], we have proved a reduction in escalation costs but it's not used across the different functions", as stated by the Engineering Trainer. However, the CS Manager stated that, in addition to CS, "Primus supports IT, specific quality assurance and Engineering personnel and a part of manufacturing use the software". Customer Support "quickly discovered that the knowledge management system enables them to spend more time on the job learning rather than searching for answers", as explained by the E-Services Manager. Making the tool available to customers for "self-help has also reduced the time needed to answer calls", as stated by the KDG Officer.

The system was created due to "falling profit margins, increasing demand for product technical knowledge (both by customers and internally), increasing complexity of products as well as number, and the rising cost of the CS", as stated by the KMS Engineering Trainer. The objective or goal of adopting a KM approach in CS is to push knowledge toward the customer as the longer it takes for a customer's problem to be solved (from the time the "call was logged"), the more layers (functions) of support it is escalated through, increasing cost and the utilisation of resources.

IMPACTS		ISS FUNCTION: NO KM INITIATIVE	CS FUNCTION: KM INITIATIVE
(1) Individual \s	Learning	Security conferences, Employee reviews as well as external reviews	Amount of time in Training before use on the job – reduced from 6 to 3 months, Employee reviews
	Adaptability	Product complexity is high & constant – K Tools	Product complexity is high & constant – CBR Tool supports the process.
	Satisfaction	Job is easier due to specific processes & tools/practices available	Access to greater number of solutions – makes job easier & is recognition of value within the organisation.
	Adaptability	Specialised group to coordinate & share knowledge across organisation.	Increased sharing across the different levels reduces cost & improves productivity.
	Satisfaction	Shared knowledge across the different groups	Customer problems are escalated through the different levels to develop new solutions
(2.1) Product / Service	Value-added	Best practices & standards are sought & evaluated to improve security within the organisation. Diagnosing of problems increases knowledge of Security groups & response times for fixes	Escalation processes enables improved service & products for customers. Reverse-engineered products (Corporate & Vendor) increased value of solutions & products
	Knowledge (based)	Fewer surprises in regular audits, increased security information & tools for customer products	Improvements on products from Customer feedback & repeated bugs are passed back to Engineering to fix in the next release. Faster response time for fixes, Pushing knowledge back to the Customer reduces costs.
		Full package inc security provided to Customers	Solutions for problems are made available to Customers.
(2.2) Processes	Effectiveness	Brainstorming sessions; Use of GW (email) & repositories of Best Practices, Standards, & lessons-learned	Employee rotation to learn from Engineers; Brainstorming sessions; Number & use of Forums, No of shared solutions published per CS member.
		Fewer mistakes made – after evaluations	Fewer mistakes made – with access to knowledge reservoirs
	Efficiency	High number of external web sources; High volume of K stored in repositories. Number & use of Forums	No of Solution hits is measured & rewarded; Reuse of Solutions
		Frequency of Calls per Customer / Employee, Use of Corporate Expert list.| No. of improvements as a result of an Evaluation	High number of external web sources used; High volume of K stored in repositories.
			Frequency of Calls per Customer, Use of Corporate Expert list, No of improvements as a result of KM or Knowledge Tools, No of hits for solution links.
	Innovation	Brainstorming for Audit reviews to improve the process & the evaluation, Group formed to use security as a selling enhancement	Innovative Solutions are pushed back to the customer to reduce costs & time required of Innovators, Improved use of internal stored & tacit knowledge
(3) Organisatio	Direct	Security strategy is aligned to business strategy	KM is not aligned to business strategy; KM is ad hoc & specific to CS. However knowledge (solutions) is pushed towards the customer to reduce CS costs.
		Membership of regulatory bodies to drive the industry	Reduction in escalations reduces costs
	Indirect	Poor security has dramatic affect on Corporate image	Enhance Customer loyalty by being open
		Best practices shared to be more effective in protecting the org.	Product designs shared in Eng. to increase productivity, Faster response than competitors

Table 5.12: IS Security and Customer Support KM Impacts.

5.1.8 Summary: Managing ISS and CS Functional Knowledge

Table 5.12 outlines the different impacts generated as a result of the two approaches used to manage knowledge within the two functions. While CS has a formalised KM initiative through the application of the CBR tool, the IS Security function benefits from the formalised processes used to manage the organisation's regulatory requirements. ISS has significantly impacted the organisation. The ISS strategy is aligned to the business strategy ensuring that ISS is mapped to every organisational technology and process. ISS is an active member of regulatory bodies and steers the market to create potential financial gains for CME-Co. An inefficient ISS function would result in corporate breaches and loss of earnings. The KM strategy used in CS is not aligned to the business strategy and as a result is dependent on the CS practitioners who are driving the use of KM tools and processes. KM is also specific to Customer Support. However CS costs are reduced and time which would have been spent answering calls by Engineers is spent creating new products. Customer loyalty is also increased when an organisation is open and willing to share knowledge. Therefore the two functions have benefited from managing knowledge. CS utilised a KM initiative to positively impact the CS function and ISS manages knowledge due to environmental requirements. However ISS has also identified market niches to target and ultimately increase profits. The functions have been positively impacted by managing knowledge. To benefit from the lessons-learned from CS the ISS function could exploit case-based reasoning tools and devise incentives for ISS practitioners to become problem-solving gurus.

The findings provided a rich description of the approaches used by the IS Security and Customer Support functions, in CME-Co, for managing knowledge and its impact on the members, functions and the organisation. While the Customer Support functions attempted to implement and manage their knowledge, the findings showed that the IS Security functions were just as effective without implementing a KM initiative. The findings also showed that the circumvention of control by the Customer Support functions has a "knock-on" effect on the IS Security function and their roles in protecting the organisations. The implementation of regulatory controls provided the IS Security functions with tools, processes, specialised roles and mechanisms to coordinate, control, evaluate and monitor functions, traffic flows, access to corporate knowledge stocks and rogue (internal and external) behaviour. It is clear from the findings that these control mechanisms, which appear to stem primarily from environmental drivers specifically impact the organisation's IS Security functions positively and the CS functions negatively.

CHAPTER SIX

EXPLORING THE TELE-Co CASE STUDY

6.0 Introduction

The preceding Chapter presented the data gathered in the first case study. The purpose of this Chapter to address the first research and the second research questions through steps 1, 2, 3 and 5 of the research protocol described and illustrated in Chapter 3 (section 3.5 and Figure 3.1). The case organisation has been assigned a pseudonym, which is a condition of the researcher's authorisation to access the organisation and conduct and publish the study as it pertains to the organisation (Figure 1.1). This Chapter consists of eight primary sections (6.1.1 to 6.1.8) to structure the case as required by the research lens (Figure 2.5 and described in section 2.7.1). Sections 6.1.1 and 6.1.2 describe the organisational background and infrastructure. Sections 6.1.3 and 6.1.4 describe the management of knowledge within the ISS and CS functions. Section 6.1.5 compares the approaches used by the two functions. Sections 6.1.6 and 6.1.7 describe the mechanisms used to promote the management of knowledge and the impacts at a functional and organisational level. Sections 6.1.7 and 6.1.8 conclude by highlighting the impact of compliance on the management of knowledge within the organisation (Table 6.12).

6.1 TELE-Co

6.1.1 Organisational Background

TELE-Co (pseudonym) is an Engineering company and a global leader in wireless, broadband and automotive communications. The organisation operates in a very dynamic industry where knowledge and learning are paramount to the development of new products. The business environment is influenced by rapid technological advancement, high demand and short product lifecycles and therefore a high level of uncertainty. Threats such as reverse-engineering, viruses and regulatory constraints are considered significant. TELE-Co's product portfolio is complex and range from wireless handsets and networks to embedded telematics systems that enable automated navigation. Table 6.1 provides an overview of the company's profile since it was formed in 1928 (Table 3.4). The organisation entered the mobile communications sector in 1936 and has since then strived to be the first to release new mobile technologies into the market. This goal is, according to the Director of HR, "driven by an innovative working environment and a highly rated Customer Support service". The corporation's mission is to leverage the collective knowledge of the global corporation through strategically utilising processes and software tools which can enhance its efficiency. The efficiency of the company's product realisation process is one of its key competitive strengths. As described by the PKM Coordinator "TELE-Co today faces the challenge of developing innovative products to build market share, while at the same time reducing the time to market, improving the total product cost, and meeting the quality, performance, reliability and value needs of our customers and markets". This drive is towards mass customisation, through "a market-of-one as well as for supply

chain efficiency", as stated by Design Engineer 1, has highlighted the need to manage product development resources efficiently and in a manner that coordinates [the many facets of] Engineering, Manufacturing, Marketing, and Distribution. The organisation has recognised the need for both a secure and a productive control environment. Knowledge is regarded as a corporate resource and according to the PKM Coordinator "significant investment has been made into establishing a global prototyping knowledge management group and in implementing ICT to support both a culture of collaboration and security". As described by the TGS Coordinator "security is considered at a senior level to be both a necessity and a key selling enhancement for new product releases". The organisation is a global organisation "with regional divisions defined by product under the World Engineering Corporation [WEC] umbrella", as stated by the Former Engineering Manager. Each division is regarded and "referred to as an organisation supported by a CS, IT and Security Support functions", as stated by the TIP Auditor.

For the purpose of this investigation the Global Telecom Solutions Sector (GTSS) is investigated. As explained by the CS Manager "cell phone support, for customers such as O², varies from [queries regarding] coding errors, product changes, interface changes and usability support". The ISS function is "charged with assuring the infrastructure of the organisation and protecting assets such as product designs and processes", as stated by the TGS Coordinator.

PROFILE OF TELE-Co	
1928	TELE-Co started as Galvin Manufacturing Corporation in 1928.
1936	Entered the Mobile Communications business with Police Cruiser Radio.
1943	First portable FM two-way radio for U.S. Army.
1955	First high-power transistor in commercial production.
1963	Developed first rectangular picture tube for colour TV.
1969	First words from the moon relayed via a TELE-Co radio
1970	Formed the Science Advisory Board Associates (SABA)
1976	Moved its Headquarters to Illinois U.S.
1983	World's first commercial handheld cellular phone.
1986	Invented the Six Sigma Quality Improvement Process. It provided a common Worldwide language for measuring quality and became a global standard.
1995	The TELE-Co pager is the world's first two-way pager.
1996	World's smallest and lightest cell phone.
2000	Wireless phone for always-on Internet access.
2003	TELE-Co announced that it would spin off its semiconductor product sector into a separate company called Free-scale Semiconductor, Inc. The new company began trading on the New York Stock Exchange on July 16th of the following year.
2004	Iconic RAZR V3 wireless phone introduced.
2005	Fast Broadband Network using a relay system.
2006	Sold its Automotive Division in order to streamline cell phone business.
2007	Sold its Embedded Communications Group to Emerson Electric Co. – provided services and products to manufacturers in Defense, aerospace and medical imaging. Closed its plant in Cork Ireland. TELE-Co had a presence in Ireland for over 20 years and has grown to the unique position as the only major supplier of both mobile communications and embedded solutions.
2008	Split into two independent companies: TELE-Co Mobile Devices and TELE-Co Broadband & Mobility Solutions, with two Co CEOs.

Table 6.1: History of TELE-Co (Corporate Documentation: Table 3.4).

With respect to this investigation, Table 6.2 provides an overview of the data gathered from multiple sources within TELE-Co.

OVERVIEW OF TELE-Co									
TELE-Co -Multinational, -Engineering -53k Employees -€3.6 Billion "07	**Industry Sector**		**Customers**		**Products**		**Competitors**		**Partners/ Vendors**
	Telecommunications Industry		Fortune 500 Companies, Vodophone, O²		Semi-conductors, Cellular Phones, Two-way Radios, Pagers, Medical Systems, Power Supplies		Nokia, Ericsson, Lucent, Samsung		Microsoft, Cisco, McAfee, Security Forums, Regulatory Bodies, Interoperability Groups
	Corporate Strategy		**Mission**		**Subsidiaries**		**ISS Function**		**CS Function**
	To be the world leader in telecommunications infrastructure and product developments		To leverage knowledge to achieve product realisation & a market of one		N. America, France, Ireland, Israel, Sweden and UK		Full function is displaced throughout Org.		Supporting regional customers
Interviews	**IS Security Function**			**Customer Support Function**			**Other**		
	Role	**Years**	**Subsidiary**	**Role**	**Years**	**Subsidiary**	**Role**	**Years**	
	• IT Manager • TGS Coordinator • Security Officer • Security Officer (Networks) • Security Coordinator • TIP Auditor • Security Officer • TIP Coordinator • Compliance Coordinator	9 7 3 4 8 2 1 5 4	Cork/EMEA U.S. Cork. U.S. U.S. U.S. Australian. U.S. U.S.	• CS Engineer • CS Eng. Manager • Design Engineer 1 • Design Engineer 2 • Design Engineer 3 • Design Engineer PKM Coordinator • DB Analyst (Compass)	12 10 5 7 3 7 9	Cork/EMEA. Cork. U.S. U.S. U.S. U.S. U.S.	• Director of HR • Former Engineering Manager • Former Project Manager	6 15 7	
Documentation Analysed	**Security Documentation**			**Customer Support Documentation**			**Corporate/Public**		
	• TELE-Co Customised – ISO17799 Documentation • Security Policies Re: email/ Internet/ Remote Access/ SID • POPI – (protect our proprietary information) • Business Continuity Procedures • TELE-Co Electronic Info. Security Standards = ISO17799+ • TELE-Co Standard Operating Procedures • Standards of Internal Control (SIC) • TELE-Co Code of Ethics • Disciplinary Measures for Policy Breaches			• Presentations: • KM Courses @ TELE-Co University • Six Sigma – A Necessary Change • TELE-Co Technology White Papers: M-Gates • Intranet: Customer Services Website • University – Online Courses: Six Sigma, M-Gates • TELE-Co Website – www.TELE-Co.com			• Annual Reports: 2000/05/06/07 • Code of Business Conduct: Our Responsibility as Employees. • Corporate Newsletters • Timeline Overview of TELE-Co History 1928-09		

Table 6.2: TELE-Co Data (Adapted from Tables: 3.3 (Roles & Responsibilities of the Interviewees) & 3.4 (Case Documentation Analysed)).

6.1.2 Organisational Infrastructure

The organisational infrastructure is the foundation on which KM resides and is composed of: organisation culture, structure, communities of practice (CoP), common knowledge and ISS infrastructure. These TELE-Co components are discussed in the next five sub-sections.

6.1.2.1 Organisational Culture

Organisational culture reflects the norms and beliefs which guide the behaviour of TELE-Co's employees. TELE-Co's culture is reported by the PKM Coordinator as a "knowledge sharing and innovative culture". The CS Manager contends that the culture "very much depends on the region, and affects the sharing of knowledge across the organisations [functions]". As explained by the Engineering CS Technician "EMEA is quite different from APAC [Asia Pacific], Europe and India are very open to sharing information or knowledge but China will forget about you as soon as you leave the country [after a meeting] and escalate calls as soon as they can [pass a problem on]". As described by the IT Manager, "TELE-Co does not have an overly restrictive environment". The TGS Coordinator further explained that "physical security is very visible and policies and ethics are evident to all employees, security is transparent and seen as a necessity given the competitive environment [the organisation] operates in". The business environment and customer requirements have forced a culture of security awareness.

6.1.2.2 Organisational Structure

Organisational structure is complex in a multinational organisation. The reporting structure can impact the management of ISS and CS knowledge. "The structure of the organisations is convoluted and we are trying to reorganise it to be more effective in supporting the business", as stated by the TGS Coordinator. Currently the organisation is divided according to "five separate [product] divisions [situated] across the globe", as explained by the TIP Auditor. Each division is under the WEC umbrella and described as follows: (1) the Broadband Communications Sector, (2) the Commercial, Government and Industrial Solutions Sector, (3) the Integrated Electronic Systems Sector, (4) the Personal Communications Sector, and finally (5) the Global Telecom Solutions Sector (GTSS). The Global Telecom Solutions Sector delivers the infrastructure, network services and software that meet the needs of operators worldwide, while providing a migration path to next-generation networks that enables TELE-Co to offer innovative, revenue-generating applications and services to customers. As explained by the CS Manager, "the GTSS is composed of Design, Development and Support Engineers with business units such as Sales, Marketing and HR and ISS functions". "The calls rotate to a local dispersed support team, then it is escalated to the next level of support and then to Design Engineering and so on", as stated by Design Engineer 2. A PKM group was "established in 2000 to support the knowledge requirements of Customer Support and Design and Development Engineering to reduce product life cycles", according to the PKM Coordinator. "The PKM group coordinates the alignment of knowledge management to existing TELE-Co processes [M-Gates]", as stated by Design Engineer 3.

6.1.2.3 Common Knowledge

Common knowledge helps integrate employee knowledge through the use of terminology relevant only to the organisation. TELE-Co's product portfolio is wide and complex requiring significant expertise in supporting customer needs. As explained by the Former Engineering Manager "product design specifications are considered common knowledge". "Methodologies developed internally, such as the Six Sigma quality system, are regarded as additional languages. Employees are taught [Six Sigma] as part of our induction programme through TELE-Co University", as stated by Design Engineer 3. As described by the [Cork] Security Officer "anything available on our corporate Intranet is pretty much viewed as common knowledge, employees have access to contact lists, presentations, policies and best practices for whatever function you are working in". "SETA is also a necessary part of our induction programme with emphasis placed on the different penalties for breaking security policies, this is an Engineering organisation and security education about common threats is necessary", as stated by the Director of HR. Therefore TELE-Co utilises common knowledge to induct new hires into an engineering and competitive culture.

6.1.2.4 Physical Environment

Physical environment is an important consideration in fostering knowledge management. As described by the [Cork] Security Officer "an open plan office is consistent across the organisation except at a managerial level and for conference rooms". "Physical security is evident but this is more for outsiders coming in. While we have to follow [restrictions such as] swipe key access – it becomes the norm after a few weeks", as stated by the TIP Coordinator. The CS Manager further explained that "it [physical security] isn't even noticeable now but I have problems with a geographically displaced support team for GTSS. Not only is time and language an issue but so is our presence for some groups. If I or a member of my team is physically present in our APAC offices; knowledge sharing is easy but as soon as we leave it disappears". Therefore geographically dispersed subsidiaries are a challenge for ISS and knowledge management.

6.1.2.5 IT Infrastructure

IT Infrastructure facilitates and supports an organisation's KM infrastructure. As explained by the PKM Coordinator, "Engineers can avail of content management systems [which store lessons-learned and documentation] that allow all employees to search for any published documents and, depending on their access rights, retrieve the necessary documentation". Therefore "employees can determine the existence of work already carried out and request access if needed", as stated by the DB Analyst. "Information systems to support knowledge capture and reuse are presently in place or being rolled out, one example is: Metaphase, a system for product data management [PDM] and configuration management [CM]" according to the PKM Coordinator. "Communication is controlled [and monitored] with technologies such as scanning devices, firewalls and secure identification cards [SID], yet the organisation thrives due to the balance between security and productivity determined as effectively as possible through trial and error", as stated by the TGS Coordinator.

Due to various legal issues TELE-Co is not a single global organisation. The organisation "requires a global security infrastructure with roles allocated to the different categories of security who collaborate through call conferencing, video conferencing, the Intranet, email and Compass which is based on a package called LiveLink[18]", as explained by the Security Coordinator. TIPs utilises "specialised hardware and software to conduct forensic data analysis to search for files related to ongoing litigation, investigative support, breaches of network security and loss of intellectual property", as stated by the TIP Coordinator.

Table 6.3 summarises the TELE-Co Organisational Infrastructure.

OVERVIEW OF ORGANISATIONAL INFRASTRUCTURE	
DIMENSIONS	**CHARACTERISTICS**
Org. Culture	• The value of KM is recognised by management but championed by a CoP - PKM • An awareness of Security but not a part of the culture ISS is transparent to users • Knowledge sharing and innovative environment • Multinational Organisation with varied cultures and languages Can cause communication problems • Knowledge sharing and innovative culture
Org. Structure	• Hierarchical structure with product divisions (GTSS) • Umbrella organisations for e.g. WEC, Security Organisation • Reorganisation in progress: constantly shifting • Communities of practice (CoP) are created for specific projects – PKM • Specialised units/divisions and roles are used – for e.g. TGS, the TIP TIP Auditor, Corporate Security Officer & Knowledge Champion (Unofficial)
Common Knowledge	• Common Engineering and Telecommunications terminology • Shared values and norms • Corporate University – for skills development, induction training & common methods
Physical Environment	• Open plan office in each subsidiary – except at a management and function level • Geographic separation between Security Officers, CS and Design Engineers • No specifically designed rooms for sharing knowledge – Teleconference rooms • Face to face contact within teams is very rare • Visible physical security presence – Guards, SID & Swipe card access, secure rooms
IT Infrastructure	• Corporate content management systems/Central repositories • Controlled, protected lines of communication: -Trial & Error approach to access • Global security infrastructure with allocated roles to each security category • Intensive forensic analysis of files across the organisation

Table 6.3: Characteristics of the Organisational Infrastructure.

The next section describes the Customer Support function's approach to managing knowledge.

[18] LiveLink is a Web-based content management system.

6.1.3 Customer Support Function

TELE-Co is "divided into separate [internally referred to as] organisations such as Security and regional divisions under WEC [World Engineering Corporation] which is a coordinating umbrella for the divisions", as stated by the CS Manager. Each is "supported by a CS, IT and security team", as expanded by the CS Engineer. The GTSS division designs, and develops cell phones, and peripheral devices. The division utilises a Customer Support team to interact with customers and Engineers. "GTSS along with its Customer Support team is dispersed throughout the world and depending on the number of Engineers in any one location – that group could have [an] IT, Security and compliance, Marketing, Sales and HR teams [assigned", as described by the Former Engineering Manager. As described by the CS Manager "the CS Team, is located throughout EMEA and APAC, so support Engineers [different levels of support] are located in Cork, the UK, Germany, India, China and Australia". "GTSS is responsible for designing, developing and supporting a wide portfolio of complex [cell phone] products [and or components]", as stated by Design Engineer 1.

Engineers are also "divided according to their role in the development of a product [or component], such as design [Engineering], product [Engineering] or development [Engineering], testing Engineers and Support Engineers", as explained by the Former Engineering Manager. This can be "further broken down by [design] domains, for example, a cell phone can have multiple parts with groups of Design Engineers working in design [knowledge] domains like interface design, coding or the [outer] casing", as stated by the CS Manager. Additionally each [design] domain has to work "separately yet simultaneously to design each part while generating a great deal of [design, test and projection] knowledge for a single product", as stated by Design Engineer 4. "It is very difficult to combine and share the knowledge generated during this process so we decided to create an ad hoc team, made up of GTSS Engineers, to coordinate the different domains and called [it] PKM", as further explained by Design Engineer 4.

The PKM team was established in 2000 and "uses teleconferences and net meetings, approximately every two weeks. It has grown to about thirty Engineers, across a range of TELE-Co organisations [including iDEN, the Commercial, Government, and Industrial Solutions Sector (CGISS), the PCS Applied Manufacturing Systems Technology (AMST) group, the Software and Systems Engineering Research Lab (SSERL), and the Compass/Desktop Solutions group]", as stated by Design Engineer 2. The Prototyping Knowledge Management (PKM) team's mission statement is as follows: to partner with product development and core process teams, to integrate design knowledge sources within TELE-Co's product realisation process. By focusing on M-gates 7 to 5 (Figure 6.1) and coordinating access to the PKM system [a document repository accessed through Compass] and other software tools, our cross-sector team will work towards significantly reducing design cycle times and total cost of ownership [TELE-Co Website].

As described by the PKM Coordinator "the team is facilitates discussions [through] forums and developing a community of practice to address the need for applying TELE-Co's best technical expertise across a wide range of projects and functional organisations". The team is specifically "addressing the need to access best-in-class knowledge, without requiring direct access to, for example, Engineers as virtual experts and virtual product designs", as explained by the Former Engineering Manager. The

PKM team is "working to integrate and leverage prototyping, knowledge management [PKM], teams, and other communities of practice (CoPs) in TELE-Co. Even though the team is essentially a volunteer effort it has grown from five [founding members] to thirty", according to the PKM Coordinator. This indicates the increasing perceived value of using PKM by additional domains and Engineers.

The following section identifies the different types of knowledge utilised by the Customer Support function.

6.1.3.1 Types of Customer Support Knowledge

The different types of CS knowledge are described in the next three sub-sections. The first section describes the general knowledge necessary for practitioners to conduct their day-to-day operations. This knowledge is categorised as general as it is available to the CS function working throughout the organisation.

General knowledge common to the CS function is specific to a "product during its design, development, implementation and support", as stated by the CS Engineer. "Corporate information, and policies are available on the Intranet through Compass, and product designs and trouble-shooting guides are available through the group portal", as stated by the CS Manager. "Any warnings about a product identified by one customer or by an Engineer are emailed to the entire support function as well as any links that might be useful", as explained by the CS Engineer. As explained by the PKM Coordinator, "Prototyping is a complex process that is familiar to everyone [across WEC]. It includes all design evaluation methods that do not require a physical prototype". However "in a broader context the process includes both tactical and strategic prototyping – it's how our innovative products are originally conceived", as explained by the Former Engineering Manager. Traditional "prototyping focuses on evaluation and improvement of existing product designs, [PKM] addresses design concept exploration, design optimisation, product platforms, product families, product behaviour emulation, requirements management and everything else", as stated by the PKM Coordinator. As explained by Design Engineer 4 "Knowledge in TELE-Co is domain [product] specific and generated through simulations, so knowledge regarding RF[19], systems, circuit simulation, mechanical CAD, hardware/software co-design, semiconductors, materials, manufacturing, and reliability, and audio quality is general in those domains". "Engineers would also regard themselves as experts on the inner workings of every area [domain] if you asked them", as stated by the Director of HR.

The next sub-section describes the technical knowledge possessed by members of the CS function.

Technically specific knowledge is specific to the CS function. "Design data is initially valuable knowledge but does end up as general knowledge posted on Compass for the support team", as explained by the DB Analyst. As described by Design Engineer 2 "design knowledge is anything associated with a design. Low-level design data is [the] raw output of simulation programs and the contents of CAD files. Design information is design data that is potentially useful for decision-making. The values of design

[19] RF: short for radio frequency, any frequency within the electromagnetic spectrum associated with radio wave broadcasts.

information are capable of being directly compared to product specifications [the estimated average talk-time or physical size of a phone]". As explained by the PKM Coordinator "design knowledge is the knowledge that is actually applied in the decision-making process". In order to be applied "design knowledge must first be defined as design information, communicated to the product designer, and then actually applied by the Product Designer in making [specific] design decisions", as explained by the Former Engineering Manager. Examples of design knowledge are "learned values of simulated talk-time and physical size of a planned portable product, which are applied by the Product Designer in making decisions during the design process", as stated by Design Engineer 4.

As explained by the CS Manager "phones are complex and so difficult to support [given the fact that] each product has a large number of interacting components. A digital cell phone can have more than five hundred parts, like: SMT [surface mount technology] components, housing, speaker, microphone, display, battery, and a keyboard, each requiring some type of support". Additionally, the CS Engineer further explained that "each element can interact with neighbouring elements in a variety of ways. For example, adjacent SMT components can interact among each other in terms of layout space, electrical routability, signal propagation delay, EMI [electromagnetic interference], as well as mechanical performance during a [physical] drop of a phone". "CS has to [therefore] support all [of] the components and the coding behind the device, which is usually a divide-and-conquer approach in figuring out what the problem is and escalating it to the right level, " as stated by the CS Manager.

The next sub-section describes the knowledge used for a particular circumstance or problem.

Contextually specific knowledge within CS is primarily used to solve customer problems [calls or fixes] and prototyping issues. Customer Support, "use design specifications to help solve product bugs" according to the CS Engineer. According to the CS Manager "we spend a lot of time trying to reverse-engineer a phone or the part my team is responsible for. If we can't solve a call, we escalate it to the Engineer responsible for coding, or interoperability – whoever is needed". "Product specifications are available through the CS and Engineering portals [accessed through Compass], as are manuals and trouble-shooting procedures", as stated by the CS Engineer. According to the PKM Coordinator "knowledge regarding a new product design changes during the design as we try new variations and test them using our different simulation models". "[Variations of designs are] recorded so that we can review the changes and a parts [display] possible interaction with another part", as explained by Design Engineer 2. "Although single-domain simulation models have been developed to understand some of [these] interactions, [the complexity] of all interactions has been beyond [both] human understanding and the limits of traditional, single-domain simulation tools", as explained by the Former Engineering Manager.

As explained by Design Engineer 1 "some simulations and analyses [testing] are restricted to a single domain [for example a drop test in the mechanical Engineering domain] and if a problem cannot be solved it can and does often affect other tests [or] other components". "[This] deficiency would still occur even if all [of the] single-domain simulations were performed [to completion] with a high level of accuracy, as the simulations still would be inadequate to predict total product performance", as

explained by the Former Engineering Manager. “To minimise design cycle time, the subsystems of new products must be designed concurrently, by focused expert design teams [each designing in a different design domain], as further explained by the PKM Coordinator. Decisions made within each team tend to affect the performance of other subsystems or components. As described by the Former Engineering Manager “if these design dependencies are not identified and controlled, the interactions can lead to design errors and product failures. Identifying these interactions is beyond the scope of single-domain simulations”. “It is our experienced Engineers who are skilled in combining the different design [outputs] from the different teams to create an integrated model [or] prototype of a new product or component”, as stated by the PKM Coordinator.

Furthermore “customer specifications collected by our Marketing organisation or from the feedback from Customer Support are [regarded as] very useful in terms of determining trade-offs during the design phase”, as stated by Design Engineer 1. As described by the PKM Coordinator “trade-offs regarding mechanical, electrical, and manufacturing domains have first to be defined, and then evaluated to produce the lowest cost and highest performance products [subject to customer specifications]”. “This [additional dimension] also lies beyond the scope of single-domain simulations and often depends on the experience of Design and Product Engineers”, as explained by Design Engineer 3.

Table 6.4 summarises the different types of CS knowledge identified in TELE-Co.

CUSTOMER SUPPORT FUNCTIONS: SUPPORT KNOWLEDGE						
Types	**General Knowledge**	**Role**	**Technically Specific**	**Role**	**Contextually Specific**	**Role**
Declarative						
Explicit	Documentation describing TELE-Co, Stock options, Org. Chart	O	A document/ report describing: Design Data from Simulations	O	A document describing known problems re: X Product	O
	Email warnings from Engineering/CS re: Errors & links to a solution	O	A document describing: Product trouble-shooting procedures	O	Feedback from customers re: product requirements	S
	Documents/reports of (a GA product) specifications	O	Reports of Simulation data & CAD Files	O	Feedback from CS Technicians re: product errors or problems	O
	Document outlining the different Domain functions and their objectives	O	Documents outlining the different interacting components of a product	O	A document/report of a new product design	S
			Document outlining the design decision-making process	O	A document describing problems re: unreleased X Product	T
Tacit	Knowledge of the Regulations pertaining to TELE-Co products	O	Knowledge of the factors to consider in comparing Domain Knowledge results (product components).	O	Knowledge of the factors to consider in determining trade-offs	T
	Knowledge of Prototyping, M-Gates.	T	Knowledge of the factors to consider when developing a new product.	O	Knowledge of the different variations for a new product	O
	Knowledge of Evaluation Techniques	T	Knowledge of the interoperability of customer products	O	Knowledge of the simulation tools	O
	Knowledge of functional/Domain Knowledge-Product experts	O	Knowledge of the different escalation levels	O	Knowledge of the limitations of single domain simulation tools	O
	Knowledge of Roles and responsibilities	O	Knowledge of coding part of a product's functionality.	O	Knowledge of the possible knock-on effect of one product/component on another	T
	Knowledge of Market/Customer Technologies	T	Knowledge of solving/ diagnosing coding error procedures.	O		
Procedural						
Explicit	A white paper describing the steps in the M-Gate methodology	O	Knowledge of the steps needed to utilise the data from simulations & CAD files	T	Knowledge of the different simulations and the ability to combine the results	S
	A white paper describing the steps in PKM	O	Knowledge of the steps in applying design data to a Design Decision	T	Sequence of steps a CS Technician uses to solve a coding error	O
Tacit	Basic knowledge of the steps necessary to apply M-Gates	T	Knowledge of the steps involved in solving a coding error or reverse-engineering	O	Knowledge of the steps in applying feedback & incorporating it into the design.	T
	Basic knowledge the steps needed to apply PKM	T	Knowledge of the steps in dividing and conquering a problem.	O	Knowledge of the steps in evaluating a design/product	T
* Knowledge Roles: Operational = O; Tactical = T and Strategic = S						

Table 6.4: Types of Customer Support Knowledge.

6.1.3.2 Reservoirs of Customer Support Knowledge

Knowledge pertaining to the CS function resides in several different locations within the organisation. They encompass people and functions, including, Engineers, Technicians, HR, management (CS, and Engineering) and groups/teams (CS, Design and Product Engineers, and PKM); artefacts, including procedures, repositories; and organisational entities, including organisational units, and inter-organisational networks. The reservoirs of knowledge are discussed in following sub-sections.

Customer Support regards **people** or practitioners within the function as its greatest knowledge source. As explained by the CS Manager "support staff are our greatest asset, they have to be up-to-date on the latest products [regarding] design specifications, coding faults and error passing [or trapping], interoperability [with vendor products, customer infrastructure] and trouble-shooting [approaches]. Without their expertise we would not be able to support our customers as quickly as we can". "Technicians [as the first-line of support] are able to retrace problems using a very old approach called: divide and conquer [to] diagnose a problem, if they can't [rectify the problem] it's escalated to the closest Level 1 or 2 support team which could be located anywhere in EMEA or APAC", as stated by the CS Engineer. "We [the regional teams] then escalate the call based on its type – the component we think is at fault or if it's a design issue [high-level coding] we then escalate it to a Product or Design Engineer", as explained by the CS Manager. As explained by Design Engineer 3 "when calls or fixes are escalated to us, and we are in the same building as the EMEA team, it's easy to work with them but if the Level 1 or 2 Support Engineer is in APAC we usually just fix the problem ourselves [without collaborating]". "Engineers are [regarded as] TELE-Co's" key asset; they are the innovators and develop our products, we provide them with as much support and leeway as possible so as not to stifle the creative process", as stated by the Director of HR. He further explained that "the HR database is a priority system here and many security controls are [aligned] to it as we keep all of the details regarding our Engineers stored on it. We not only keep details [regarding] their designs but also [regarding] how they actually work so that we can allocate appropriate people to their teams or train them to work effectively with these key Engineers who are usually managers". As described by the IT Manager "a significant number of [security] controls are added to the HR database [PeopleSoft, Oracle DB] because our Engineers are headhunted and you don't want Nokia to have access to profiles of our Engineers as well as our designs". According to the PKM Coordinator "Design and Product Engineers are experts in their product ranges and we can utilise them more if we allow them to collaborate across the organisation".

Groups are created to support particular products. TELE-Co uses the term organisation for specific functions within the company such as the Engineering organisation or the IT, Security and compliance organisations. As described by the Director of HR "Customer Support consists of support Engineers who are our front line defence or provide support to our customer-base, Design Engineers are split into teams according to the different products such as GTSS which is wireless and anything in communications". "[We also have] Product Engineers, who take the design and build the actual product, combining the different component [domain] designs and the trade-offs, which is then tested and hopefully the first to market", as explained by the Former Engineering Manager. As explained by the PKM Coordinator, "Design Engineers are

experts in their fields with significant knowledge of [the] TELE-Co product portfolio and their components as well as those of our competitors. They can diagnose or retrace any design problem and apply a cross-team approach to the design process by using our internal M-Gates process". "The PKM team was created to utilise their experience more productively and collaborate across the different design domains to ultimately improve the process and the realisation of the first-to-market goal", as further explained by the PKM Coordinator. As explained by the CS Engineer "each [design domain], for example radio frequency Engineering, Mechanical Engineering, Manufacturing Engineering, typically performs at least a few basic simulations within its domain and an overall team, like PKM, combining those processes could increase productivity but it isn't supported by senior management". "Members of the team are purely there on a volunteer basis and while it's a good idea they have to prove its monetary value to WEC", as explained by the Former Engineering Manager. Another group used as a source of processing knowledge by the different Engineering groups is the CMPR (Concept to Manufacturing Process Redesign) team. As described by the PKM Coordinator, "CMPR created the M-Gates process, as a part of their initiatives in the areas of system and product development (SPD) and market and product line planning (MPP)". "The M-Gates process [or framework] has been implemented by GTSS, CGISS, PCS, and other associated [business] groups", as stated by Design Engineer 2. "The objective of the CMPR team is to improve product and system time-to market and business predictability", as stated by Design Engineer 3. As described by the CS Engineer "CMPR advise everyone, especially the design and development groups how to apply M-Gates so that they are all using the same process". This approach is used to standardise the management of projects within TELE-Co.

Knowledge is **stored** in **artefacts** such as practices, technologies and repositories. **Practices** can be organisational routines and procedures. As explained by the CS Manager "CS uses a number of routines and procedures in solving calls, When a customer such as O² calls its local support a ticket is created through our tracking system, which is the beginning of the procedure. If a Technician cannot point the customer to a solution or fix, the call is escalated to Level 1 and 2 and so on. During each escalation the work or coding is recorded in a trouble-shooting document which we review and reuse". "We do need a type of system to effectively allow [us] to create, store, share and reuse our solutions; we are just recording them in Compass for now", as stated by the CS Engineer. "Everything in TELE-Co is documented in some sort of template to be signed-off and stored, primarily due to corporate policy. We do use approaches in trouble-shooting and a coding process but the more experienced [Technicians] tend to take short cuts in using the different processes and recording solutions; but we are getting better at it", as explained by the CS Manager. As explained by Design Engineer 2, "M-Gates is our version of a best practice approach for designing a new product. It's divided into phases or gates and each phase forces us to document the result which might be requirements or test results [outputs]". "Prototyping is a methodology which allows the design teams to follow specific steps [simultaneously] and document the results for each model", as explained by Design Engineer 2. "Product specifications must also be documented as part of M-Gates and versions [levels of detail] of this document are released to our customers, Customer Support and stored with WEC", as explained by Design Engineer 1.

A considerable amount of knowledge is stored in TELE-Co **technologies** and systems. "Compass is the internal repository which operates as part of the corporate Intranet", as

stated by the DB Analyst. “Employees and groups can use it as an Intranet to post and access documentation and presentations, or at a deeper level it can be customised to share group-specific material like trouble-shooting manuals”, as explained by the CS Engineer. According to the CS Manager “repositories are used to record our calls and solutions; these are reviewed internally by the support team but we also use Compass and regional shared drives for sharing solutions”. “Vendors provide us with access to their product specifications or solutions [as] customers use other products as well and sometimes the problem can be caused by interoperability issues”, as stated by the CS Manager. As described by the PKM Coordinator “computer simulations can predict product behaviour before physical assembly. These [simulations] are an integral part of Engineering”. “Simulations are performed to reduce cycle time, to aid in understanding the behaviour of complex systems, to improve designs, and reduce production risk”, as explained by the Former Engineering Manager. “Design tools are used at different stages of the M-Gate process. CMPR provides simulation models and support services, for example, electrical circuits [analogue, digital, mixed-signal, RF] and mechanical assembly. CAD tools are also used to model the processes and aspects of the prototype as a record for a gate”, as stated by Design Engineer 1. According to the PKM Coordinator “a set of web pages have been created in the TELE-Co document repository Compass which contain a list of members, and short summaries of projects related to PKM. The web pages also include links to repositories like meeting minutes and the reference library. The library is constantly being updated by PKM team members and covers categories like best practices, communities of practice, creativity and innovation, knowledge management, TELE-Co core process redesign examples, TELE-Co software tools and guidelines, and industrial applications for tools we use like CAS [Complex Adaptive Systems]”.

Knowledge is also stored within **organisational entities**. “M-Gates activities are cross-functional and require an integrated team effort”, as stated by the PKM Coordinator. The PKM team works closely with the CMPR team during the design process and for access to information useful for evaluating product designs”, as stated by the Former Engineering Manager. As described by the CS Manager “besides Product and Design Engineering we work with Marketing, IT and Security. Engineering support us in solving calls and IT provide our IT services. Security set up direct links with our customer-base. They also have to allocate access to the different systems that we use or want to develop for internal use”. “Marketing work with our customers in selling our products. We have to help Marketing by acting as Technical Advisors because they wouldn’t understand the technical aspects of our products, and they provide us with feedback from the customers”, as stated by the CS Manager. Additionally, “Engineering collaborates with marketing in preparing brainstorming sessions and sales pitches to customers”, as explained by the Director of HR. “Technical knowledge is currently not shared with other business units due to a lack of understanding of TELE-Co products”, as stated by the CS Engineer.

TELE-Co collaborates with partners and customers to form mutually beneficial **inter-relationships** and to ensure customer platform independence and manufacturing standards. “Engineering in TELE-Co utilise a direct line of communication with customers, for example O², over a virtual private network (VPN) to debug errors”, as stated by the Security Coordinator. According to the CS Manager “the connection is restricted to Engineering to prevent an inexperienced employee from modifying code”. As explained by the PKM Coordinator “developments in simulation have been reported

at many TELE-Co symposiums, where we [Engineers] have the opportunity to meet with other Engineers and swap knowledge regarding our approaches and design issues". "The symposia allows the company to participate or lead the industry by its involvement in leading simulation software developments, regulations regarding standards – which is the way to stay ahead in this industry", as explained by the CS Engineer. "We have established a connection with a government-sponsored resources [such as the] repository to extract Green component advice in making our products more environmentally friendly", as stated by Design Engineer 2. Finally "online forums hosted and run by TELE-Co Engineers are used to help other Engineers, students or anyone interested in SW Development, it's also used to collaborate on programming errors", as stated by the CS Engineer.

Knowledge resides in several reservoirs within the organisation, which are summarised in Table 6.5.

CUSTOMER SUPPORT FUNCTIONS: RESERVOIRS OF KNOWLEDGE	
People:	
Individuals	• CS Specialists (Table 6.2 provides an overview of the different Engineering Experts) • Technicians – Product specifications, Coding faults, Trouble-shooting • Level 1& 2 Support Engineer – Problem-solving • CS Engineer – Problem diagnosing • Product or Design Engineer – Design the product range • CS Manager – Coordination of the regional teams • IT Manager/Security Officer – aligns security controls • PKM Coordinator: Promotes the use of KM across the Engineering Domains
Groups	• Regional Teams – Support teams based in EMEA and APAC. • Customer Support (Engineers) - Support Customers • World Engineering Corporation - Coordinating umbrella for the Product Divisions • Engineering: Develops products & reverse-engineers competitor products. • GTSS Engineers – Cell Phone Division |Product Domain Engineers • PKM (Ad hoc) Team – Products, M-Gates & Prototyping
Artefacts	
Procedures	• Problem-solving routines & procedures – Step-by-step guides for tackling calls • Escalation procedures – requires collaboration with the required expert • Templates – recording solutions • Trouble-shooting Documents – To solve problems • Coding process – Step-by-step divide & conquer procedure • Corporate policies – Compliant procedures for documenting processes & responsibility • M-Gates – Design best practice approach • Prototyping – Methodology for testing prototype designs • Document process – Recordings of product specifications
Repositories	• Compass – Corporate repository of Manuals, Presentations, everything • Group Website (Compass) – Documentation, Trouble-shooting manuals, Best practices • CS Repository (Ad hoc) – Records Calls & Solutions | Regional Share Drives • Vendor Repositories – Product specifications • Documentation Management System (DMS) – Procedures • Government Sponsored Repository – Extract Recommendations |Online Forums
Technologies	• Simulations – Design data | CAD Tools – CAD Designs
Org. Entities	
Organisation	• Organisational Infrastructure (Table 6.3)
Units	• Marketing – Collect Customer feedback & Technical Advisors to Marketing • IT Organisation – Provide IT Support & Services • Security & Compliance – Provide Secure Connections to for e.g. Customers • Core Process Redesign Team – M-Gates process • U.S. Engineering – Call Escalation
Inter-organisational Relationships	• Vendors – Product specifications/Market standards • Product interoperability problems & Feedback re: Trade-offs | Debug Customer Errors • TELE-Co Symposia – Engineering Industrial Collaborative Forum • Participate in the Development in Mobile Standards & Regulations • Government – Extract Requirements re: Environment Design Considerations • General Public – Programming Errors

Table 6.5: Reservoirs of Customer Support Knowledge.

6.1.3.3 Customer Support KM Processes

This section describes the processes used to support the acquisition, capture, creation, sharing, application and control of knowledge in Customer Support.

The **acquisition** of knowledge within TELE-Co is not common. The M-Gates framework was "developed internally but has been utilised by other companies; we do collaborate through our TELE-Co symposia but unless we need guidelines regarding regulations we usually develop everything in-house", as stated by the Director of HR. As described by the PKM Coordinator "the M-Gate framework is a high-level process for product development". Figure 6.1 is an illustration of the TELE-Co M-Gate process with its five phases and fifteen gates. Knowledge is acquired through regular conferences which enable the organisation to collaborate with industry and academia.

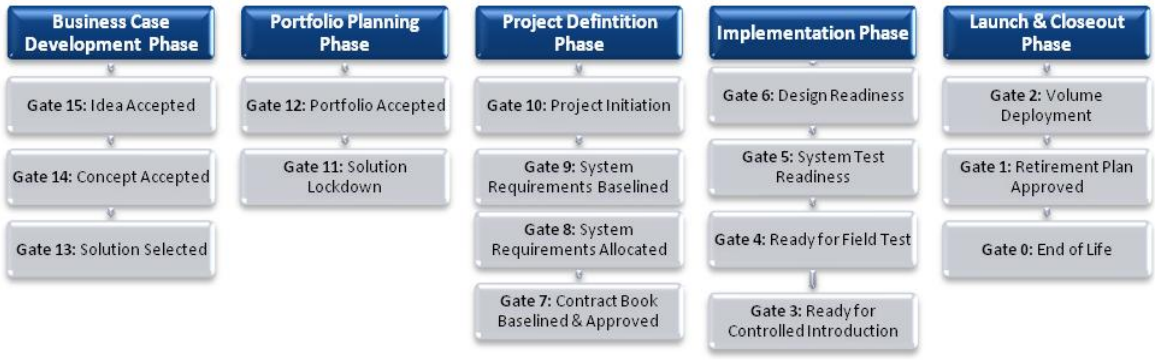

Figure 6.1: TELE-Co M-Gate Process.

Knowledge is **captured** or retrieved from the numerous simulation repositories used in Engineering "to build models or review previous tests", as stated by Design Engineer 2. As explained by the PKM Coordinator, "Compass is used as a central repository for any and all guidelines needed for Engineers. It is also an access point to other repositories owned and maintained by other teams like CMPR". Customer Support pulls knowledge from the different repositories described in sub-section 6.1.4.2.

Knowledge is continuously **created** and **shared** through the problem-solving and M-Gates processes. "Engineering does use M-Gates for product realisation. It leverages the collective knowledge of the company through strategically targeting processes and software tools to enhance efficiency", as explained by the Former Engineering Manager. According to the Security Coordinator "the [M-Gates] process provides product development milestones which do incorporate security considerations as part of the overall development process". "TELE-Co [specifically Engineering] is driven by the realisation of the corporate product process as a competitive advantage, as time or first-to-market is the goal of the development process", as stated by the CS Engineer. "As design cycles become faster, learning cycles become faster, thereby enabling better execution of product introduction plans". Each stage of which is risk assessed in terms of cost and failure", as explained by the PKM Coordinator.

As explained by Design Engineer 1, "M-Gates is a divide-and-conquer standard that we can all use across the organisation from Engineering to IT. It is really used to make sure

we are all consistent in our approaches to problem-solving". "Each phase or gate forces an output from the team, such as a case for the development of a new product, a proposed solution, then approval from cross-domain team leaders and a Security Advisor to testing results and simulations", as stated by Design Engineer 2. "M-Gates forces the creative process and collaboration of a design team not only for a specific component but across the different design domains each sharing the different designs and test result outputs. Sometimes advisors from other departments are needed, like security if for example we have to work with a partner and a secure connection is required", as stated by Design Engineer 3. As explained by Design Engineer 2 "sharing of design documents is easy using systems such as email, Compass and mentor graphics [a CAD tool]; we also use teleconferencing and face-to-face meetings".

Knowledge is **applied** throughout the different phases and gates. According to the PKM Coordinator simulation modelling [as required by M-Gates] can help drive design and innovation, decision-making processes and knowledge reuse and capture". Requirement number 3 for M-Gate 8, states that simulation must be performed, "but there are no guidelines for what simulation is required or how the tests should be preformed", as stated by Design Engineer 2. "The basis for decision-making processes and knowledge reuse and capture and, in a larger sense, all aspects of the M-Gates framework, is knowledge. [Therefore the] management of knowledge through the M-Gate framework is vital to [the successful] execution of the framework", as explained by the PKM Coordinator. M-Gates also forces a "holistic approach to the design process by requiring the design teams to re-evaluate the process", according to the Former Engineering Manager. "The design specifications created by the design teams are stored and distributed through Compass", as stated by the CS Engineer. As explained by the CS Manager "Customer Support has limited access to product designs, code and known bugs". "We use trouble-shooting guides from different sources, mostly internally, and try and solve customer calls; a fix really depends on the different support teams" ability to diagnose a problem and reverse-engineer the product", as stated by the CS Manager. As explained by the CS Engineer "we use a divide-and-conquer approach to problem-solving; a problem is escalated through different support levels until it's fixed". "Work is shared as the problem is escalated and we do try and store solutions for future use. At the moment everything is stored in Compass but it isn't a knowledge management system", as stated by the CS Manager. As explained by the CS Engineer "teleconferences, Compass, email and face-to-face meetings are our primary ways to share and reuse solutions".

Knowledge **control** is necessary to assure the validity and utility of knowledge. "Security is applied in protecting product designs through access control lists which are decided by Engineering", as stated by the Former Engineering Manager. According to the [Cork] Security Officer "secure connections are used for establishing connections with customers, partners and off-site support teams for GTSS". However "the primary control for Engineers are legal documents requiring non-disclosure of our trade secrets and we have enforced this [through penalties] with former [Engineering] employees", as explained by the Director of HR. As described by the CS Manger "they [Security] apply controls and we have to fill-in SRD [security requirements documents] forms when developing a database or requesting a secure connection but really we only contact them when the network or a system is down".

Table 6.6 summarises the CS knowledge management processes.

CUSTOMER SUPPORT FUNCTIONS: KM PROCESSES	
Processes	
Acquisition	• TELE-Co Symposia – Regulations, Market and Guidelines • Reverse-Engineer competitor products to determine their product design
Capture	• Simulation Models – Product Designs, Data, Test Data • TELE-Co Reservoirs of Knowledge (Table 6.8) accessed through: Compass – Procedures, Product Specifications & Manuals • Roles & Responsibilities for the Escalation Process
Creation	• Problem-solving Process – for the creation of a Design or a Solution • Trouble-shooting Guides – Created by CS Team Members • M-Gates Process – for Product realisation & documentation • Product Development Milestones – Deliverable at each stage or gate • Security Considerations – Added to the product Design • Product Introduction Plans – Produced • Divide & Conquer Approach – Each problem is broken down into smaller problems • Risk Assessment – Risks are identified – e.g. Costs and Trade-offs • First to Market Product – End result • Approval Process – Cross domain/team approval of each design component • Security Evaluation – Results of Product Testing for security considerations.
Sharing	• Creation Process – Every Output is shared between the Domain Teams • Problem-solving – solutions are shared across the Regional Teams • Email, Compass, Teleconferencing, and CAD Tools – Design Documents • Product Designs – Customer Support Teams (limited access) • Code & (known) Bugs – Customer Support Teams (limited access) • Trouble-shooting
Application	• M-Gates – Each Gate requires the application of knowledge Decision-making, holistic approach to Design | Incorporates an Evaluation Phase • Simulation Modelling – Drive designs, innovation, decision-making process • Design Reuse – through Simulations, Gates, and Prototyping • Solve Customer Calls – through Experts and stored solutions • Diagnose Problems – through Problem-solving • Reverse-engineering – to solve problems • Escalation Process – to solve problems Teleconferences, Compass, Email, and Face-to-face collaboration • Stored Solutions – for reuse
Control	• ACL: Access Control Lists are used to control access to Product Designs • VPN: Virtual Private Networks are used to encrypt communication tunnels • Legal Documents – NDAs are used to control Engineers re: sharing & selling designs • SRD – Security Environment Document to identify security requirements • Engineering – Decide access and use Security as a support function

Table 6.6: Customer Support KM Processes.

The next section describes ISS function's approach to managing knowledge.

6.1.4 IS Security Function

TELE-Co Global Security (TGS) function "is dedicated to providing security and loss prevention services both internally and externally to customers and employees [alike]", as stated by the TGS Coordinator. "The Corporate Security function is recognised throughout the world as a group of experts with in-depth experience and knowledge in the security industry", as stated by the Director of HR. As described by the [Networks] Security Officer "they have built a solid structure designed to resolve risks by improving [ISS] processes that ensure a secure infrastructure for employees through proactive security strategies [policies, secure technologies and business assessment methodologies]".

"Due to policies like POPI [protect our proprietary information], TGS reduces loss and damage to corporate property and supports employee productivity by maintaining a secure control environment", according to the Compliance Coordinator. The organisation's internal security function is based in the U.S. "TIP [TELE-Co Intellectual Property group] is separated into six sectors each focusing on a different technology and self-contained", as stated by the [Networks] Security Officer. According to the IT Manager "Corporate TIP rolls down the policies regarding the protection of information. It is responsible for investigating, reacting and recommending technologies to each GEO [subsidiary]". "In fact the businesses are so diverse that one factory could be more concerned with physical security than another where information security is of a higher priority", as stated by the Security Coordinator. As a result TIP is divided into divisions to "ensure that every aspect of security is covered but it's not integrated", as stated by the TIP Auditor. The divisions are as follows: (1) policies, (2) tools, (3) compliance, (4) incident investigation, (5) recommendations, and (6) crisis management [TELE-Co website].

As described by the TIP Auditor "TIPs are responsible for developing global [TELE-Co] security procedures and policies which are disseminated to the various GEOs [subsidiaries] who customise the policies for use as some controls, especially in an international company such as this, like encryption tools [levels] can be used legally in the U.S. but cannot be exported to other countries". "The TIP organisation follows two standards SIC (Standards of Internal Control) and EISS (Electronic Information Security Standards) or ISO17799 as a guideline or checklist to secure the assets of the multinational", according to the Compliance Coordinator. "The primary difference between the use of these standards is the degree to which they are internally enforced", as stated by the [U.S.] Security Officer. "The standards are suppose to be followed by every employee in the company and are used as internal self-assessments for the organisation", as explained by the [Cork] Security Officer. According to the TIP Auditor, "once every three years each subsidiary is audited by corporate TIPs to determine the degree to which they adhere to the standards or [security] documents [checklists]". "They each [subsidiary] follow local policies, process documents [templates] and procedures to ensure compliance", as stated by the Compliance Coordinator. The report will either document a failure or a pass for the subsidiary. "If they fail they are re-audited within six months", as stated by the [Cork] Security Officer. However, this fact is contradicted within the ISS function, that is, some Security Officers stated that "TIPs are stringent in enforcing audits, [others stated that] it varies – depending on I suppose the profile of the site [which could be a manufacturing plant or an R&D centre]". As explained by the TIP Auditor "an audit is

an intensive and time consuming process, as long as the subsidiary makes the recommended changes and meets the JP Morgan's review - we are happy". JP Morgan is used as a compliance consultant as well as the official audit reviewer for TELE-Co. Each corporate sector assigns an individual as a Security Officer who "spends [his/her] time completing one or more or parts of an audit, such as for example disaster recovery or physical and electronic procedures", according to the Compliance Coordinator. "The IT function supports each division [and in this organisation GTSS] using the same security policies", according to the IT Manager. "GTSS is located throughout three regions and is supported throughout the world", as stated by the CS Manager. "There is a single point of contact [usually an assigned Security Coordinator] within the different sectors who share knowledge through emails and conference calls", as stated by the IT Manager. "Sixteen [IT] staff are located in the Cork team, all of whom follow different security policies, for example building machines [security control requirements] to reviews [audits]", as stated by the [Cork] Security Officer. The primary activity conducted by the ISS function is the "electronic tracking of employees [in WEC] through the use of SID and network monitoring software", as stated by the TGS Coordinator. The network is continuously scanned "to check for breaches in security and to ensure that internal users are not allowed to access restricted information or knowledge", as stated by the [Networks] Security Officer. This activity or process is limited to prioritised internal corporate networks such as the Engineering domains "due to the cost of the activity and the priority of Engineering compared to other business functions", as stated by the Security Coordinator.

6.1.4.1 Types of IS Security Knowledge

This section identifies the different types of knowledge utilised by the ISS function. The different types of ISS knowledge are discussed in the next three sub-sections. The first section describes the general knowledge necessary for ISS practitioners to conduct their day-to-day operations. This knowledge is categorised as general as it is available to all IT professionals working throughout TELE-Co. Section 6.1.2 described the culture, ISS structure and common knowledge used in the organisation, all of which is regarded as general knowledge by the interviewees. It is fundamental to the function's knowledge of roles and responsibilities at corporate and local levels.

General knowledge common to the ISS function is varied. As explained by the Security Coordinator "TELE-Co utilises the ISO17799 standard with the objective of covering all aspects of information security so therefore: the security policy; organisational security; asset classification and control; personnel and physical security; communications and operations management; access control lists; systems development and maintenance; business continuity planning and compliance – it pretty much covers everything". "Knowledge of security technologies, [current] threats, and risks are also [regarded as] basic security knowledge", as explained by the [Cork] Security Officer. Initially regulatory knowledge was categorised as technical knowledge by the function but "today regulation knowledge is part of our online training [portfolio available through the TELE-Co university] and we all have to know about compliance", as stated by the [Australian] Security Officer. "Policies, procedures and a good understanding of the organisation is also important now so that we [ISS function] know what's important instead of just letting management identify assets – sometimes they don't know what's [connected to] a part of the network", according to the [Networks] Security Officer. As described by the TIP Auditor "templates such as the SRD [security requirements

document] and AAG [access administration guide] should be considered general knowledge once filled-in". The templates are used by the different business functions "to identify security requirements", or the "resources needed from Security for a project", as stated by the [Cork] Security Officer. The SRD [security requirements document] provides "the place [template] for the Project Managers to indicate how the requirements [and resources] were met", as stated by the IT Manager. The AAG is designed to document access administration procedures to maintain adequate security for each system or process.

"Checklists are used to control internal operations, we have checklists for everything such as: assessment criteria's for ASPs [active server providers], other providers [NSP], best practices for secure development and anything to do with our external operations - primarily", as stated by the [Networks] Security Officer. The [Australian] Security Officer further explained that "they [checklists] will always be used – auditors and management like them but there are too many of them and they are used just once or perhaps edited for the next time". As explained by the [Cork] Security Officer "control checklists are very useful and common, we use them for all of the information systems – it seems silly but we need them and use them as an inventory of servers, routers, tunnels [VPN], different security technologies that are connected to the network, otherwise we just wouldn't know [what is connected to the network]". The [Networks] Security Officer added that "even in TELE-Co some employees – we'll say for example Engineering can bypass our controls and add unsecured boxes [servers] causing problems in terms of risk [backdoors] to the corporate network".

The next sub-section describes the technical ISS knowledge possessed by members of the ISS function.

Technically specific knowledge is specific to the ISS function. The purpose of the ISO17799 is to define and establish a consistent set of ISS controls which are required to protect TELE-Co's information or knowledge assets and intellectual property (IP). As explained by the Compliance Officer, the standard "is categorised as technically specific knowledge once "it is customised and it is reused over and over again". Audit reports are documents "generated by the internal audit committee under TIPs", as stated by the TIP Coordinator. "If a group or subsidiary fails the [audit review] document can be used to learn from the mistakes made and rectify them for the next audit", as further explained by the TIP Coordinator. According to the TGS Coordinator "participation in regulatory bodies enables us to evaluate the best practices available and utilise them in the organisation". "Log files from our firewalls, VPN monitoring software, IDS and scanning tools like Black Ice provide a wealth of technical knowledge about our network", as stated by the [Networks] Security Officer. According to the TGS Coordinator "we monitor and track everything our employees do as well as rouges – rouges are our biggest threat".

"Scanning tools allow us to track any rouge activity but they are also [used by hackers in] scanning our network for vulnerabilities [network backdoor]", as further explained by [Networks] Security Officer. "Security companies are used [either by TGS or the external auditor] to perform network penetration tests in order to evaluate our network security controls", as stated by the TIP Coordinator. The security company provide ISS with "a report documenting any and all weakness", as explained by the [Networks] Security Officer. Vendor sites provide "technical and troubleshooting manuals on their

products", as stated by the Security Officer. Forums such as "the Irish Security Forum [ISF], the international forum, CIO surveys, [emailed] vulnerability alerts contain valuable knowledge regarding other companies" security problems and environmental threats", as stated by the [Cork] Security Officer. As explained by the TIP Coordinator, "security conferences are a great source of papers regarding for example: the latest security issue, the security market, academic research describing organisational issues and evaluations of the different vendor technologies, we [TELE-Co] hold an international conference on security through our university every year so that we can participate in moulding the market".
The next sub-section describes the knowledge used for a particular circumstance or project.

Contextually specific knowledge within the ISS function is primarily used to adhere to regulatory issues or for incidents such as a security breaches. As described by the TIP Coordinator "specific knowledge is required on compliance and the different standards and best practices available". Auditors [external] conduct "an extensive review of our security controls [formal, informal, technical], network security and everything needed to ensure that we are complying with, for example, SOX; the ramifications of not being compliant are enormous so we source as much knowledge as we can on compliance and the effect of using different security technologies [such as encryption]". "We try and use [the feedback from the last review] to guide the steps we should take – it does get easier", as stated by the Compliance Officer.

Knowledge regarding incidents is also regarded as useful. "Rouges behave [a] certain way and we try and use our [documented] lessons-learned from previous incidents to build profiles of viruses, rouge or hacker behaviour on the network as well as recovery procedures. We are trying to be more proactive and actually be more aggressive", according to the [Networks] Security Officer.

Table 6.7 summarises the different types of ISS knowledge identified in TELE-Co.

IS SECURITY FUNCTIONS: SECURITY KNOWLEDGE						
Types	**General Knowledge**	**Role**	**Technically Specific**	**Role**	**Contextually Specific**	**Role**
Declarative						
Explicit	Documentation describing TELE-Co, Stock options	O	A document describing an Audit, Log files from Firewalls	O	A White Paper describing regulatory issues.	O
	Organisational chart, contact lists, presentations	O	A document describing the multinationals security policies	S	Standards & best practice documentation	O
	Servers, routers inventory list	O	A document describing a penetration test	O	ISS Audit reports	T
	SRD Template	O	A document describing the ISS Strategy	S	Incident reports	O
	AA Guide – filled in	O	Security alert reports	O		
Tacit	Knowledge of Security technologies, threats and risks	O	Knowledge of the factors to consider in evaluating security controls.	T	Auditor's knowledge of regulations, standards and best practices.	T
	Knowledge of regulations	O	Knowledge of the factors to consider when evaluating security technologies	S	Security Officers knowledge of different risks and vulnerabilities	T
	Knowledge of systems on the network	O	Knowledge of Domain (Function) access requirements	O	Auditors review of Security controls	T
	Knowledge of TELE-Co Roles and responsibilities/Domains	O	Knowledge of scanning tool report indicators	T	Auditors knowledge of complying with SOX	O
	Knowledge of ISO17799 procedures	O	Knowledge of Security Forums and the security market developments	T	Knowledge of impact of using different security technologies	O
Procedural						
Explicit	Checklists: for internal operations	O	ISO17799 – section describing policies	O	Document outlining the sequence of steps in applying lessons-learned.	T
	Security policies	O	A manual describing troubleshooting procedures	O	A Security Officer's knowledge of steps needed to use (Audit) feedback.	T
Tacit	Steps in identifying security assets	O	Security functions knowledge in applying the lessons-learned from an Audit	T	A Security Officer's knowledge of steps in incident recovery	T
	Basic knowledge in the steps for assessment criteria	O	Security functions knowledge of the steps necessary to evaluate security best practices	T	Knowledge of the steps to identify rouges and hackers.	T
	Basic knowledge in reusing checklists	O	Security functions knowledge of the steps necessary to prioritise vulnerabilities	O	Knowledge of the steps needed to react to rouges	T
* Knowledge Roles: Operational = O; Tactical = T and Strategic = S						

Table 6.7: Types of IS Security Knowledge.

6.1.4.2 Reservoirs of IS Security Knowledge

Knowledge, pertaining to the TELE-Co ISS function, resides in several different locations within the organisation. They encompass people and functions, including, IT and Security professionals, Engineers, management and groups/teams within ISS; artefacts, including best practices, security technologies, and repositories; and organisational entities, including organisational units, organisations, and inter-organisational networks. The organisation reservoir is the TELE-Co organisation in its entirety. This reservoir of knowledge is described as part of the organisational infrastructure in section 6.1.2. The remaining reservoirs of knowledge are described in the following section.

A considerable amount of knowledge resides in **people**. As described by the TGS Coordinator, "experts are allocated to the different corporate security requirements such as network security, WEC, auditing, compliance, intellectual property and the different GEO offices". Additionally, "an Export Manager is assigned to each site to make sure that everything [product or SW licences, encryption] moving from one [office or facility] region to another is checked by the manager so that TELE-Co does not break any International or U.S. laws", as stated by the Security Coordinator. As explained by the IT Manager, "a Compliance Coordinator was hired to make sure that we know and do everything we are supposed to do". "Policies, best practices and standards are rolled out by the [Compliance] Coordinator who evaluates them for TELE-Co", as explained by the TIP Auditor. "Audits [initially] were very time consuming but our internal committee coordinated by a TIP Auditor provides useful reviews and general assurance that we will comply with any and all of the regulations", as explained by the TGS Coordinator. As described by the IT Manager, "the Security Officers are assigned regions and have enormous responsibilities in ensuring that these regions meet TELE-Co security needs and they could be physically hundreds of miles away". "They [Security Officers] need to be on top of all the risks we face and the controls we need to work effectively", as stated by the TGS Coordinator.

The structures of the different **groups** working within the ISS function is described in section 6.1.3. The different groups, including TGS, TIPs, Networks and IT operate individually and collectively. However, the groups "interact primarily though email, which is difficult to manage and find [existing] solutions to calls when needed again", as stated by the [Cork] Security Officer. "Reporting is also difficult as each Security Officer reports to the site IT Manager but is structurally aligned to the Corporate Security group", as explained by the IT Manager. "TIP is responsible for providing the regulatory guidelines for all of TELE-Co, they are the go-to group for all things compliance", as stated by the Security Coordinator. According to the Compliance Officer, "TGS manages the entire security organisation through the Security Officers; it isn't what would be viewed as a two-way relationship as the Security Officers provide TGS with status reports and TGS instructs the [security] officers in rolling out patches for example", as explained by the [Networks] Security Officer.

Knowledge is **stored** in **artefacts** such as practices, technologies and repositories. **Practices** can be organisational routines and procedures. As described by the Security Coordinator, "the ISO17799 standard is used as a guide or procedure in protecting every aspect of security", as stated by the Security Coordinator". As explained by the

Compliance Coordinator, "procedures such as: disaster recovery and continuity plans are regularly updated and stored in the security repository [through Compass]". Adherence to SOX and other regulations "is vital and steps are identified to adhere to audit requirements, which are continuously updated before, during and after internal and external audits", according to the TIP Coordinator. According to the Security Coordinator, "depending on the procedures or guides in question we will store [them] in multiple locations [databases, shared drives, websites and repositories] which are integrated through Compass". "Alerts and guidelines on their [TIPs] internal website but normally they send us whatever they want us to implement", as stated by the [Cork] Security Officer. Therefore the function stores security practices and procedures in different repositories.

A considerable amount of knowledge is stored in TELE-Co **technologies** and systems.

"Vendor sites are particularly useful as practitioner's sources of manuals, patches and troubleshooting documentation", as stated by the [U.S.] Security Officer. Security technologies are also used to provide security members with technical knowledge such as log files. Data is pulled through and filtered by security databases. As explained by the Security Coordinator "[security] technologies generate a lot of technical knowledge, and it is difficult sometimes to mine through to find the alert". "We filter the data from the different firewalls, IDS software and scanning tools into a database so that we can summarise what's going on in the network", as explained by the [Networks] Security Officer. However "these [technical] controls and steps are used to protect the WEC networks leaving the other business functions without as many controls to monitor, which is a weak points", according to the [Networks] Security Officer. As described by the [Cork] Security Officer, "there are numerous tools and security technologies in TELE-Co that we need to do our jobs". He further explained that the different technologies are categorised by use "by the group, ourselves and by the company – email and Compass are used to collaborate on different projects, incidents or something like an audit, but I would use my customised portal for storing my documents, papers, and checklists – I use Excel for everything, particularly [reused] lists and identifying variances in scans. We also use logs generated by scanners, servers, and firewalls to provide us with knowledge of the corporate network". Excel is used extensively throughout the organisation; "the group uses spreadsheets automatically [programmed to] calculate the level of risk [or vulnerability associated with a particular system] and produces a brief summary of risk for TGS", as stated by the [Networks] Security Officer.

The [Networks] Security Officer identified "scanners [as] the ultimate resource for networks, scanners perform scans of [to monitor]: the data centre, the Intranet, Extranet and employees". He further explained that "we have separate scanners for each of the systems that I mentioned and they identify high, low and medium vulnerabilities in detailed reports for us". "The findings and trends are reported to our system administrators through ART [the automated analysis, reporting, remediation and tracking tool). System administrators are responsible for implementing fixes to remove any vulnerabilities identified", as stated by the Security Coordinator. Scanners are also used to generate a view of the TELE-Co network "by scanning selected IP addresses and the results are correlated into a central vulnerability data repository", as stated by the [Networks] Security Officer. The data repository "allows TIPs to generate reports to describe the security health of the TELE-Co network as a whole as well as create

specific vulnerability reports for system and network administrators", as stated by the TIP Coordinator. "ART is used to track the vulnerability remediation process. Attacks like CodeRed[20] and Nimda[21], travelling through email and the web, can and do breach firewalls which means that our entire Intranet connected devices need to be secured. We use scanning and mitigation to limit TELE-Co's internal exposure by examining our current information infrastructure and determining what is required to assess our internal vulnerabilities on a continuous basis", as explained by the [Networks] Security Officer.

Knowledge is also stored within **organisational entities**. These range from the entire organisation, units within the organisation and **inter-organisational** relationships. The organisation as a whole is described in section 6.1.2. The culture, structure, values and practices are discussed and summarised in Table 6.3. TELE-Co outsources to "application and Internet service providers for website hosting, business processes and managed services, [TELE-Co] must ensure that its vendors can provide an acceptable level of security as part of their business practices", as stated by the Security Coordinator. Risk analysis procedures are used by ISS to determine a potential partner's level of security. Additionally TIPs is a contributing member of ISF [the International Security Forum]. "ISF is composed of seventy-five to eighty-five member organisations that are based in a variety of countries and operate in sectors such as financial services, information services, manufacturing, advisory services, retail, transport and energy", as stated by the TIPs Coordinator. "The forum generates [security] papers with direct applicability to the information security issues troubling TELE-Co [as well as its other members]", as stated by the [Cork] Security Officer. As explained by the Compliance Coordinator, "JP Morgan and Deloitte provide invaluable feedback from the audits conducted and surveys produced". Regulatory bodies are "useful sources for the best practices used in the industry", as stated by the TGS Coordinator.

The ISS function also collaborates with other **functions** within the organisation. It interacts with "primarily WEC (the World Engineering Corporation), they are prioritised by headquarters, most of our controls are aligned with Engineering networks which obviously makes the business functions weak-links and they shouldn't be", as stated by the [Networks] Security Officer. According to the TGS Coordinator, "the [security] organisation works with every department [or organisation] in TELE-Co. Project leaders have to document using, a SRD [Security Requirements Document], what [security] resources they need and an assigned Security Officer will determine the risks of, for example, another repository and ensure that the right access has been aligned". "TELE-Co employees are also expected to participate in audits and ensure that their departments adhere to security policies", as stated by the Compliancy Coordinator. He further explained that "Finance and HR also collaborate with us, the CFO signs-off on audits and is involved in determining access for employees to different repositories and HR enforces penalties for breaches of security when we produce proof of an employee's inappropriate traffic accessing sites [through individual scans]", as stated by the Security Coordinator.

Knowledge resides in several reservoirs, which are summarised in Table 6.8.

[20] CodeRed: is a computer worm that proliferates on Microsoft operating systems and causes widespread Internet slowdown.
[21] Nimda: is a computer virus with a mass mailing worm which spreads quickly.

IS SECURITY FUNCTIONS: RESERVOIRS OF KNOWLEDGE	
People:	
Individuals	• ISS Specialists (Table 6.2 provides an overview of the different experts within the case) Network of experts/problem-solving for internal & external security • IT Manager – understanding of regions meet corporate IT and Security needs • TGS Coordinator - identifies corporate security requirements • Security Officer (regions) – responsible for site security • Security Officer (Networks) - network controls • Security Coordinator – Corporate view • TIP Auditor /TIP Coordinator – provides reviews • Compliance Coordinator – best practices and standards • Export Manager – Site product, encryption or SW licences
Groups	• ISS function – IT Services • TGS – strategies and development initiatives • TIP – pool of experts on standards and best practices • Networks – IT Services and guidelines • Corporate Security Group • Security Officers – Domain Knowledge
Artefacts	
Procedures	• ISO17799 & Compliance procedures – U.S. and International • POPI (protect our proprietary information) • SIC & EISS Standards • Security Checklists • Audit Review Reports • Disaster recovery & Continuity plans • Security practices & procedures
Repositories	• Documentation – IT/Security solutions or fixes • Portals – Customised by individual and group • Vendor sites – External sources of patches, manuals and solutions • Database – Capturing log files, scanning reports • Vulnerability Data Repository • TELE-Co Intranet
Technologies	• Compass – Content management system • MS Outlook – Problem-solving but filtering & retrieving knowledge stored is difficult. • MS Excel – Levels of risk calculator • ART – Tracking tool • Network Scanning Tools (Authenticate users when accessing resources) – Tracking Employees & Rouges & – Vulnerability Testing
Org. Entities	
Organisation	• Organisational Infrastructure (Table 6.3 provides an overview of the organisations knowledge)
Units	• Joint Projects – Domain specific requirements for X project • Business functions (WEC) Domain specific requirements, group access, roles and responsibilities, critical systems. • HR – Enforce security policies
Inter-organisational Relationships	• Partners (vendors) – joint expertise in providing security procedures • Regulatory Bodies – best practice • Auditors – Reviews, lessons-learned and guides • ISF – External collaboration

Table 6.8: Reservoirs of IS Security Functional Knowledge.

6.1.4.3 IS Security KM Processes

This section describes the processes used to support the acquisition, capture, creation, sharing, application and control of knowledge in the ISS function.

The **acquisition** of knowledge within ISS is common. "Key assets are identified, prioritised and appropriate controls are then aligned", as stated by the [Networks] Security Officer. TELE-Co acquired the ISO17799 standard "to utilise as a methodological, stepped approach in assuring the security [C.I.A] of information, data and IP [intellectual property]", as explained by the TGS Coordinator. The standard "is customised by TIPs [TELE-Co Intellectual Property group] and covers known security threats to our internal assets. The purpose of the TIPs group is to control, through policies and procedures, the ISS requirements of the different GEOs [subsidiaries], to adhere to regulatory requirements and to deliver a unified security approach", as stated by the TIP Coordinator. As explained by the Security Coordinator "SecSDLC [Secure Systems Development Life-Cycle] covers all aspects of information security [from the definition of] the security policy [to stipulate that security is aligned to the goal of the organisation], asset identification [the identification of key knowledge repositories], personnel, physical, communication security and security measures, like access controls, the re-evaluation and maintenance of security and [finally] business continuity". "Standards and policies are licensed or purchased, if they are suitable for us, but then they are customised as TELE-Co standards", as explained by the Compliance Coordinator.

Knowledge is **captured** or retrieved from the numerous reservoirs distributed throughout the organisation (sub-section 6.1.3.1). As stated by the Security Coordinator the function "collaborates primarily by phone because we are spread across the organisation". Every system, Intranet, database and [for example an audit] process "is assigned a security expert to ensure that everything is monitored and that everyone knows who is responsible for [a] resource". "If there is an incident we try to record everything [profile of behaviour] and sit down afterwards to figure out what the scanners can tell us and what to do the next time", as stated by [Networks] Security Officer. "We have a group portal in Compass where we store and retrieve all of our operational procedures and trouble-shooting guides", as explained by the [Cork] Security Officer. As explained by the [Australian] Security Officer "reams of data are collected by the TELE-Co scanners, they are programmed to collect different levels of vulnerability risks, incidents and provide information and recommendations [through a filtering databases and a pre-programmed Excel matrix] on how to summarise incidents for management". The function also "searches for [trouble-shooting] guides on different architectures being adopted and their impact on security", as stated by the IT Manager.

Knowledge is continuously **created** through the problem-solving process used within ISS. "Once every three years each subsidiary is audited by corporate TIPs to determine the degree to which they adhere to standards and [security policies] procedures. They each follow local policies, process documents and procedures to ensure compliance", as stated by the TIP Auditor. As described by the Security Coordinator "an audit report is generated at the end of the process, with everyone feeding results into the document". The review report will either document a failure or a pass for a subsidiary. "If they fail they are re-audited within six months. Each corporate sector [product division] assigns an individual as a Security Officer who spends of his time completing one or more of

the audits [such as for example disaster recovery or physical and electronic procedures]", as explained by the TIP Coordinator.

However "if there is a crisis [such as a security breach], the cost of the incident is not measured essentially because it is too hard to assess. Lessons-learned or knowledge of the crisis and the steps taken to recover are saved and **shared** through TIPs to be used for the next threat to TELE-Co", as stated by the TIP Auditor. "Data [regarding] the business impact in time and delays in fixing a system or downtime for a customer application is stored. Loss of productivity in the time it takes ISS practitioners to combat a security breach is not measured", as stated by the Security Coordinator. As explained by the IT Manager "the time allocated [by employees] is the overtime worked to pull the company back on track [after a security breach] unless the site is a manufacturing outlet with deadlines to meet".

As stated by the [Cork] Security Officer "email, Compass and teleconferences are the main tools used to share knowledge [regarding] standards, regulations, sources [for example external threat lists], and guides". "TELE-Co also leads a symposium of similar organisations to discuss the future of the security industry for improving our products but also to determine the type of [security] technologies we will need to incorporate, and future issues", as stated by the TGS Coordinator. "We are also active members of ISF where we, as well as eighty odd companies, discuss and share our [security] experiences with other Security Officers as a type of collaborative effort, since 9/11 [due to the infrastructure ripple effect of the tragedy]", as explained by the Security Coordinator.

Knowledge **application** or use is extensive in ISS. As stated by the [Networks] Security Officer "security uses everything at our disposal to give a full a picture as possible of the security health of TELE-Co". "Knowledge pulled from our security technologies is collected, stored, retrieved and analysed by the group", as stated by the TGS Coordinator. "Manuals, standards, trouble-shooting guides, policies, vendor specifications and email warnings from TIPs, Microsoft or SANs are customised and refined with use", as stated by the TGS Coordinator. The auditing process enables "TELE-Co to evaluate the internal security processes across the different GEOs; we have to coordinate the generation of a report for the external auditor as a group", as stated by the TIP Auditor. This evaluation "allows us to reuse the knowledge gained from a previous audit as well as the feedback [outlined] in the review report, which is very useful as we are given a list of things to improve [in a given time frame]", as stated by the TIP Coordinator. As explained by the [Australian] Security Officer "audits are time intensive but the review is almost like a review of [security] us for Corporate, it certainly makes us more visible to the organisation". Therefore management and ISS function regard an audit as an approach to measure the value of security to the organisation.

Knowledge **control** is necessary to assure the validity and utility of knowledge. Security in TELE-Co is applied through the use of a "three pronged approach covering network security, consisting of typical security technologies such as firewalls, VPNs, bastion servers, SID, automatic virus updates and network monitoring software, all of which impact the management of knowledge", as stated by the Security Coordinator. He further explained that "if our controls are too restrictive then the productivity of the company will be reduced – the trick is finding that balance and the only way is through

trial and error". As explained by the [Networks] Security Officer "users are tracked so we can see if someone is trying to access a system they shouldn't be or looking for specific information". "Network security is considered very transparent to internal users and facilitates the communication network for our Engineers", as stated by the [Networks] Security Officer. As stated by the Compliance Coordinator "tunnelling [VPN] is used to protect our innovative network but this can be problematic as well because as you pass international virtual borders the level [of Encryption] has to increase and it [data, information or knowledge] can then be difficult to retrieve".

"Ownership of knowledge artefacts [solutions] in repositories is controlled by the authors and access can be requested by email to the individual who created and owns the artefact", as stated by the [Cork] Security Officer. "Reverse-engineering of products is a significant threat [to TELE-Co] and first to market or the creation of a market of one is one of our goals. We as a result allocate a lot of controls to our key [Engineering] repositories", as stated by the Security Coordinator. As explained by the Director of HR "repositories and databases in HR are allocated effective security controls and monitored by network scanning software, as knowledge of expert skill-sets is a key asset and potential threats such as head-hunting key developers is a risk to KM within TELE-Co".

However, according to the Security Coordinator, "we do experience difficulty controlling Engineering groups who [ultimately] circumvent security controls in the pursuit of innovation". "Engineers require and have full control over boxes [servers] and remove and add them to and from the corporate network as desired", as stated by the [Networks] Security Officer. Therefore Security Officers are constantly "battling with Engineering to adhere to the standards and guidelines", as explained with the Security Coordinator. As described by the TGS Coordinator "groups have implemented internal demilitarised zones (DMZ) as a separate control environments for developers but full control of demilitarised zones has caused serious network breaches resulting in the unavailability [at times] of parts or all of the [corporate] network", as further explained by the Coordinator. Failures such as these are considered by Security to be "a barrier to the innovative process and [a significant] waste of resources in fixing the fault and loss of productivity due the unavailability of knowledge assets to [other] groups. "Unfortunately, Engineering have far more political support [at senior management level] but security is often sacrificed for the business case", as stated by the TGS Coordinator. Senior management view this as a necessary sacrifice "so as not to interfere with the innovation process", as stated by the [Networks] Security Officer.

"External connections [any connection between a TELE-Co network and a partner are difficult to secure and require a very substantial investment in hardware, software and administrative time", as stated by the [Networks] Security Officer. According to the Security Coordinator "log files, and operating system security issues must be monitored continuously and fixes implemented immediately". "Potential rogues or intruders probe [scan] TELE-Co's Internet connections for weaknesses every day. New types of attacks occur within several hours of a vulnerability being discovered and [successful attacks] are then published on the Internet for other hackers or to embarrass the company", as explained by the Security Coordinator. Managing an external connection "requires advanced skills, state-of-the-art security technology, and a strong commitment of time and resources. [Therefore] a security boundary must be maintained between the TELE-Co corporate network and external networks to protect the corporate network and

resources", as stated by the TGS Coordinator. "The [external] connections are managed through a control process. The process outlines how TELE-Co establishes a network connection with the Internet or a business partner, joint venture, contractor, consultant, contract manufacturer, [an] ASP, distributors, and compliant partners", as explained by the [Australian] Security Officer. To promote consistency across the Corporation; "standardised security exhibit [an NDA] was developed by a cross-functional team. [It is] by holding our vendors accountable for their security practices [that] we can better protect TELE-Co's brand equity in the marketplace", as stated by the Compliance Coordinator.

Table 6.9 summarises the ISS KM processes.

IS SECURITY FUNCTIONS: KM PROCESSES	
Processes	
Acquisition	• Regulation Guidelines – bought and customised to comply with environmental laws • ISO17799 Guideline – Purchased and customised • Sec-SDLC - Purchased and customised
Capture	• TELE-Co Reservoirs of Knowledge (Table 6.5) • Pool of Experts – security technologies and practices • MS Outlook – for collaborating and filtering • Corporate repository – documentation, procedures
Creation	• Problem-solving Process - solutions • Auditing process – Checks and balances • Audit – Trial and Error Learning Process • Lessons-learned – from current and previous reviews
Sharing	• Problem-solving – Sharing knowledge to solve and problem or fix • Incidents – Collaborating through groups to solve the problem • Coordination - through Security Coordinator • Email, Compass, TELE-Co Intranet, Teleconferences • TELE-Co Security Symposia for sharing with Academics and Security Professionals • Active participation – in regulatory bodies • ISF – Collaborating with other companies
Application	• Use of security technologies, experts and processes for integrated view of Security • Reuse of customised standards and practices • Auditing – forces documentation and lessons-learned • Reuse of solutions/fixes • Pool of Experts – use develops through trading • Use of Audit process in raising the Security groups profile • Email warnings – prioritised and carried out
Control	• Alignment of controls • Automatic virus updates • Testing of controls to prevent an unproductive environment • Network security – protect communication • Scanning of network to protect groups – Engineering • Tunnelling – applying encryption to cipher transmissions • Author Ownership of knowledge artefacts • HR repositories and databases - allocated effective security controls

Table 6.9: IS Security KM Processes.

The preceding sections depict the IS Security and Customer Support functions operating within TELE-Co. The different types of knowledge used by the functions are described, reservoirs of knowledge pinpointed and the processes used to manage knowledge by the functions illustrated and summarised in Tables 6.1 to 6.9. The next section compares the approaches used by each function to manage ISS and CS knowledge.

6.1.5 IS Security and CS Functions Managing Knowledge

This section considers TELE-Co's IS Security and Customer Support functions approaches to managing their knowledge. It extends the descriptions discussed in the preceding sections by comparing the approaches used. The different types (Table 6.10), locations (Appendix F), and knowledge processes (Appendix G) are compared and then contrasted. Next, the mechanisms used to promote the management of ISS and CS knowledge are described in section 6.1.6. These are categorised as technological and non-technological. Use of the different KM tools is outlined and illustrated to determine individual and function usage (Table 6.11). Finally section 6.1.7 concludes with a description and discussion of the impact gained due to the management of knowledge on the (ISS or CS) individual, functions (products/services, processes) and the organisation (Table 6.12). Furthermore display matrices are utilised to illustrate functional characteristics, differences and outcomes for each of the variables described. Each display matrice was reviewed and verified by the Security Officer, PKM Coordinator, and CS Manager (Table 6.2).

6.1.5.1 Types of Functional Knowledge

This sub-section summarises the different types of knowledge utilised by the TELE-Co's IS Security and Customer Support functions. Table 6.10 is adapted from Tables 6.4 and 6.7. Table 6.10 summarises the different types and roles of knowledge used by the two functions to illustrate the similarities and differences. ISS (Sec) and Customer Support (CS) knowledge (K) are categorised as: general, technical and contextually specific knowledge. These are then further subcategorised as declarative (explicit/tacit) or procedural (explicit/tacit). The roles of each type are identified in Table 6.10 as operational (O), tactical (T) and strategic (S). Role totals are calculated from Tables 6.4 and 6.7 and used to compare the importance of each type of knowledge to each function (for example general operational knowledge has a ratio of Sec K= 15: CS K=9).

General knowledge is used for day-to-day operations within the functions. The ISS function regards the following as general (operational) knowledge: organisational charts, which outline the general roles and responsibilities of the different business units, hardware (HW) specification, templates, and contact lists. Customer Support also regards organisational documentation and HW specifications as operational knowledge. However, email notifications and domain specific knowledge was identified by the function as operational. ISS regards expertise in regulations, security technologies, systems, networking and threats as operational. Procedures such as ISS checklists, policies and assessment criteria's were all identified as operational general knowledge. CS identified the steps in implementing M-Gates and PKM as operational. However, while ISS did not categorise any of its general knowledge as tactical or strategic, CS identified their expertise in and application of prototyping, the M-Gates methodology, customer technologies and PKM as tactical (Sec K= 0: CS K=5). While neither function view their general knowledge as strategic (Sec K= 0: CS K=0), CS did view its

application of development and project management methodologies as tactical. Therefore the CS function has identified the importance of expertise in applying step-by-step approaches to problem-solving due to the necessity to combine and coordinate the outputs (solutions) of different (design) domains and teams.

Technical knowledge is specific to either function. CS views its technical knowledge in designing new products as operational. ISS views alerts, procedures and evaluation reports as operational. Knowledge pertaining to domains (access rights and designs), for the functions, while requiring expertise, is categorised as operational (Sec K= 7: CS K=13). ISS regards external forums, security controls, scanning and audit reports as tactical. CS views the ability to use CAD files and design data from multiple sources (design domains) in designing a new products as tactical knowledge (Sec K= 5: CS K=2). Therefore CS views its expertise in combining knowledge from different Engineering domains as vital as it is needed to build TELE-Co products. However it is interesting that problem-solving is not viewed as tactical but operational due to the fact that "it's normal for us, we solve customer problems every day, it's what we do", as stated by the CS Manager. ISS views security policies, strategies, and regulations as strategic knowledge. The function also regards expertise in evaluating security technologies as strategic. However the CS function does not view its technical knowledge in diagnosing solutions or product design as such (Sec K= 3: CS K=0). This can be attributed to the alignment of ISS to the TELE-Co corporate strategy and the implications of non-compliance to environmental regulations. CS goals are not explicitly aligned to TELE-Co's corporate strategy.

Contextually specific knowledge was viewed as operational by the two functions. Regulations and best practices were considered operational knowledge by ISS and code errors as operational CS. CS also viewed errors, design variations and solving errors as operational (Sec K= 5: CS K=6). Contextually specific knowledge such as audit reports, lessons-learned, the reactive ability of ISS experts and procedures were categorised as tactical by ISS. Examples of tactical knowledge, for ISS, were identified as regulatory procedures, best practices and lessons-learned from audits and reactive strategies. Trade-off factors and the ability of Engineers in applying customer requirements to the design of new products were categorised as tactical by CS (Sec K= 9: CS K=5). The differences in the ratios can be attributed to financial implications of not having the necessary knowledge and expertise in applying regulatory controls, lessons-learned from audits and the inability to recognise internal and external risks. Incorporating customer feedback and trade-offs knowledge into product development is important as it would affect sales. Finally, ISS does not regard its contextually specific knowledge as strategic. However, CS categorised product designs, as well as the combined knowledge from the multiple domains, as strategic (Sec K= 0: CS K=3). This was due to the importance of engineering expertise in combining the knowledge of different domains in creating an integrated solution. This was also compounded by the fact that current simulation models cannot integrate multiple component designs. Thus, the development of innovative products is dependent on experts.

In summary the totals outlined in Table 6.10 indicate that ISS and CS knowledge is equally viewed by the two functions as operational (Sec K=27: CS K=28). ISS knowledge was viewed as slightly more tactical than CS knowledge (Sec K=14: CS K=12). The two functions regard their knowledge equally strategic (Sec K=0: CS K=0). However CS regarded its contextually specific knowledge as strategic. ISS viewed

regulatory technically specific knowledge as strategic. The totals illustrated a significant difference, within the functions, between the different roles of knowledge. ISS regard the allocations of controls and problem-solving as operational, the application of regulatory requirements as tactical and ISS policies and strategies as strategic (Sec K= 27 O|14 T|3 S). The importance of ISS knowledge can be attributed to the alignment of ISS policies and strategies to that of the organisations. The categorisation of the functions tactical and strategic knowledge is environmentally driven. The ability to identify and react to rogues (hackers) is also viewed as strategic, emphasising the functions recognition of its expertise in rectifying security incidents. However proactive strategies were not identified by the function as an important skill indicating the functions inability to be proactive in fighting attacks. The CS function can and does combine knowledge from different sources to solve problems. It was evident that the function categorises its internal expertise as strategic. The function primarily solves customer problems and categorises its knowledge as a result as operational (CS K= 28 O|12 T|3 S). Incorporating customer requirements and feedback into product design did highlight the importance of this knowledge in developing products that are practical and meet customer demands.

Table 6.10 summarises ISS and CS Knowledge.

ISS AND CS FUNCTIONAL KNOWLEDGE												
D:E/T |P:E/T		**IS SECURITY KNOWLEDGE**	**ROLE**				**CUSTOMER SUPPORT KNOWLEDGE**	**ROLE**				
General Knowledge	D:E	Org. Documentation| Charts| Contacts	O			D:E	Org. Documentation| Chart| Contacts	O			
	D:E	Security HW Lists| Template	O			D:E	Warnings| Specifications| Domains	O			
	D:T	Regulations| Technology| System| Threats| Roles	O			D:T	Regulations| Experts| Roles	O			
	D:T	Networks| Domains| Procedures	O			D:T	Prototyping| M-Gates| Customer Technology	T			
	P:E	Checklists| Policies	O			P:E	Steps: M-Gates & PKM	O			
	P:T	ID Assets| Assessment Criteria	O			P:T	Apply: M-Gates & PKM	T			
			O	**T**	**S**			**O**	**T**	**S**		
		Totals:	15	0	0		**Totals:**	9	5	0		
Technically Specific	D:E	ISS Policy| Strategy| Regulations	S			D:E	Design Data| Trouble-shooting	O				
	D:E	Audit| Alert & Evaluation Report	O			D:E	CAD Files| Processes| Prod. Parts	O				
	D:T	Domain Access Rights	O			D:T	Domain Results| Development. Process	O				
	D:T	Controls| Scanning| Forums	T			D:T	Product Interoperability	O				
	D:T	Evaluation of Technologies	S			D:T	Escalation Process| Diagnosing	O				
	P:E	ISO17799 | Trouble-shooting	O			P:E	Use of CAD Data| Design Data	T				
	P:T	Audit Reviews| Best Practices	T			P:T	Coding Errors| Reverse-engineering	O				
	P:T	Prioritise Vulnerabilities	O			P:T	Divide & Conquer Approach	O				
			O	**T**	**S**			**O**	**T**	**S**		
		Totals:	7	5	3		**Totals:**	13	2	0		
Contextually Specific	D:E	Regulations| Standards| Practices| Alerts	O			D:E	Product: Problems & Requirements	O				
	D:E	IS Security Audit Reviews	T			D:E	Unreleased Product: Problems	T				
	D:T	SOX| Impact of Technologies	O			D:E	Product Designs	S				
	D:T	Regulations| Practices| Risks| Controls	T			D:T	Product: Variations| Simulations| Limits	O				
	P:E	Steps: Lessons-learned| Audits	T			D:T	Trade-off Factors| Interoperability	T				
	P:T	Steps: Identify & React to Rogues	T			P:E	Steps: Coding Errors	O				
						P:E	Combining Domain Results	S				
						P:T	Applying Feedback| Evaluations	T				
			O	**T**	**S**			**O**	**T**	**S**		
		Totals:	5	9	0		**Totals:**	6	5	3		
		ISS Knowledge Totals:	**27**	**14**	**3**		**CS Knowledge Totals:**	**28**	**12**	**3**		
***Declarative (D)/ Procedural (P), Explicit (E)/ Tacit (T). | *Roles: Operational (O), Tactical (T) Strategic (S).** ***Totals are calculated from Tables: 6.4 and 6.7.**												

Table 6.10: IS Security and Customer Support Knowledge (Adapted from Tables: 6.4 and 6.7).

6.1.5.2 Functional Knowledge Reservoirs

This sub-section describes the different reservoirs of knowledge utilised by TELE-Co's IS Security and Customer Support functions. Appendix F is adapted from Table 6.5 and Table 6.8. The table summarises the similarities, and differences between the IS Security and Customer Support reservoirs. The third column is derived from identifying the different reservoir characteristics from the two functions. The knowledge reservoirs of the functions are categorised by their practitioners, functions, artefacts and inter-organisational relationships. These different stores or reservoirs of knowledge are discussed in the following sub-sections.

(1.) The knowledge residing in **individual** practitioners of a function can be identified through the roles and responsibilities attributed to them. Problem-solving specialists are used by the functions to diagnose problems. Managers (ISS and CS), armed with project management and policy expertise, are used to coordinate the day-to-day operations of the functions within specific subsidiaries or regions (EMEA/ APAC).

ISS utilises domain specific experts to target different aspects of IS Security. The TGS umbrella function, through a coordinator, identifies the ISS requirements of the multinational, which can be difficult given that one subsidiary (a manufacturing factory), could just require physical security while another plethora of ISS controls. Security Officers, based in and with the responsibility for specific sites roll-out informal, formal and technical controls. Security Officers are also used as experts in each aspect of security from communications network to information. Network experts are used to assure security of the corporate network which crosses over different geographic areas. They encrypt and monitor the communication network utilised by TELE-Co. Coordinators are used to ensure that Security Officers have the necessary resources, knowledge (for example regulatory) to apply the directive from the Corporate Security group (TGS). Internal auditors are used to allocate the required regulatory controls. Auditors evaluate and review corporate security. Lessons-learned are generated by audit experts to aid sites and the entire organisation in order to be more prepared for an external audit.

An Export Manager is used as a knowledge gateway for the different geographically dispersed TELE-Co subsidiaries. Each subsidiary is required to adhere to different U.S and international laws. This is particularly pertinent to technological multinationals dependent on utilising encryption (with or without VPN tunnelling) as a component of a product or for internal and external communication. Each country and or region stipulates a specific level of encryption and as a result multinationals can easily break these laws communicating between different parts of TELE-Co's communication network. Export Managers use encryption and regulatory knowledge to ensure that site encryption, software licence encryption levels for products and network points comply with regional laws. The CS function assigns experts to different (escalation) support levels. Expertise in product development, interoperability knowledge and diagnostic skills are valuable assets. Therefore the utilisation of experts, for problem-solving, operating at a high level of support diverts knowledge away from product design and development. CS Engineers are used in creating product designs, to diagnose fixes, level (1 and 2) Technicians provide front-line support to customers by coding faults and trouble-shooting

problems. A PKM Coordinator (a design Engineer) is used on an ad hoc basis to promote the use of KM in prototyping new products and designs.

It is from the above descriptions of the different roles and responsibilities within the two functions that the following characteristics were identified: escalated levels of expertise, trouble-shooting specialists, coordinating activities, diagnostic expertise, regulatory coordinators, innovators, and regional management (Appendix F: Row 1).

(2.) The managers of the two different **functions** are responsible for identifying policies, standards and procedures. TGS is responsible for formulating and developing security strategies for TELE-Co. Security Officers, as a group, coordinate the roll-out of controls across the subsidiaries and collaborate on activities such as audits particularly in preparing for them and conducting post-mortems after the process has ended. A Corporate Security group coordinates the global ISS operations. TIPs acts as a pool of compliance experts selecting and customising standards and practices. Network (NW) experts provide services and control expertise. The IT departments provide the infrastructure and services necessary for the different business functions to operate.

CS utilise an umbrella group to coordinate the different Engineering divisions. The GTSS division provides expertise regarding every component and aspect of Cell phone design and development. CS Engineers support and develop the different Cell phone components and the end products. Support Engineers (including regional teams) provide diagnosing expertise in supporting the needs of TELE-Co customers. PKM is an ad hoc community of practice composed of Design Engineers determined to combine the different design domains of knowledge through the use of KM and the project management methodology M-Gates. The primary difference between the two functions is that CS uses an ad hoc community of practice to promote the management of knowledge and ISS purchases and customises its procedures.

It is from the above descriptions of the different groups and teams interacting with the two functions that the following were identified: regional coordinating teams, strategic development, pool of expertise, measuring assessors, overview group, domain/functional expertise, product/service evaluators, cross-functional team: prototyping (Appendix F: Row 2).

(3.) Knowledge is stored in practices, organisational rules, routines and **procedures**. Document management systems (DMS) are used to control the quality of the solutions created within the two functions. ISS acquires numerous procedures externally and customises them to suit the needs of the organisation. ISO17799 is an ISS guideline that is used to provide step-by-step guidelines in protecting the organisation. Internally produced standards are also used. POPI (protect our proprietary information) is used to control employee behaviour in terms of protecting TELE-Co specific knowledge, particularly pertaining to product design. ISS checklists are used to track jobs done regarding particular projects or activities. Audit reviews are regarded as valuable sources of knowledge as they are externally sought evaluations of the ISS function. Review reports have been used as lessons-learned and a form of to do or checklist for additional audits. Business continuity plans (BCP) and best practices are externally sourced by the global security function. Procedures are customised as TELE-Co policies and

plans for internal security activities in protecting the organisation from known risks.

CS utilises templates and procedures to create uniform solutions for effective filtering and searches. This ensures that solutions can be shared, reused and tagged for CBR searches. Trouble-shooting guides are vital (if regularly updated) in order to force Technicians to follow step-by-step procedures in solving problems. This is an attempt to ensure that steps in, for example, coding are not bypassed. Bypassing steps in trouble-shooting can cost additional time if a call is escalated to another level of support. The next level of support will not be able to retrace the steps already taken. Therefore a systematic approach in problem-solving can ultimately save time. The use of a guideline enables the different support levels to collaborate as each other in coding or trouble-shooting.

TELE-Co policies dictate the documentation of processes as a prerequisite for different regulations (for example segregation of duties). M-Gates, as a collaborative project management mechanism, was developed internally to also ensure that each TELE-Co function utilises a common strategy for managing and collaborating on function-based, cross-functional and external projects. It is essentially a common project management guideline and (gate) vocabulary reference model to ensure organisational consistency across projects. Prototyping as a methodology is used throughout CS and Engineering to test new designs and to learn from failures as well as successes.

The primary difference between the functions, when retrieving knowledge from procedures, is that ISS externally sources and customises procedures to comply with environmental regulations and are dependent on checklists for completing reviews or any other ISS activity. Procedures are also used to control the behaviour of TELE-Co employees. Penalties for breaking corporate procedures are outlined and reminders are used to ensure employee compliance. Methodologies are used by CS. However they are created internally to comply with TELE-Co standards in approaching problems and building products.

It is from the above descriptions of the different procedures used by the two functions that the following were identified: best practices and procedures, planning, problem-solving techniques, escalation procedures, standardised templates, solutions, divide and conquer approach to problem-solving, corporate policies, project management methodologies, prototyping, document management systems (DMS) for managing corporate and functional documentation (Appendix F: Row 3).

(4.) Knowledge **repositories** can be paper-based or electronic. The two functions use paper-based document management systems to create standardised solutions and guides. Portals, Intranets and shared drives are used to store documents, solutions, corporate policies, by function or across the organisation. Vendor repositories are also used to source manuals regarding security technologies, guidelines for recovering from security incident or product specifications in solving inter-operability problems in a customer's environment. ISS uses the knowledge pulled from repositories to create a picture of the organisation's security landscape. Repositories are used to automatically pull (multiple) firewall, scanning and IDS logs located throughout the corporate network in order to collate filtered knowledge into a prioritised list of issues for Security

Officers. CS use manually entered logs and solutions to track customer issues and solutions. External knowledge is also pulled from government repositories to comply with, for example, green regulations in product development. CS uses public online forums to share coding solutions as an initiative to attract potential employees in the form of IT and Engineering graduates. Therefore ISS uses security repositories to automatically generate knowledge and CS uses repositories to build and store solutions. External collaboration is also sought by CS in product development to comply with external regulations and also to use external experts in coding designs.

It is from the above descriptions of the different repositories used by the two functions that the following were identified: documentation management systems, collaborative forums, central repositories, external vendor sites, databases for extracting security data such as vulnerabilities, and government sponsored repositories (Appendix F: Row 4).

(5.) Knowledge is stored in firm specific **technologies**. Email is used as a collaborative forum in problem-solving, accessing internal and external documentation and for storage throughout TELE-Co. ISS use Excel to create checklists and in calculating levels of risk for TELE-Co systems. Risk is calculated so that the appropriate level of control is determined. Scanning technologies, such as ART and Found-stone, are used to monitor the corporate network and track employees and rouges. CS exploit simulation software and CAD tools to create models of new products and test designs. Simulations are not used by ISS to create and test decision-making in simulated scenarios. Modelling is used by CS to identify different scenarios and plan for potential anomalies in design. This could also be used by the ISS function.

It is from the above descriptions, of the different technologies used by the functions, that the following were identified: collaborative forums (email), comparative analysis tools (Excel), tracking tools (for rogues), and decision-making tools (Appendix F: Row 5).

(6.) Knowledge is also stored within **functions** representing the individual stores of knowledge specific to the **unit**. TELE-Co procedures such as the SRD stipulate the involvement of a Security Advisor for projects and determine the level of security risk has been identified. The roles and responsibilities of every TELE-Co employee are outlined due to regulations (such as SOX). It is the responsibility of the ISS function to allocate or assign access to TELE-Co systems and knowledge resources based on the roles and responsibilities of employees and business functions. The HR department is responsible for identifying roles and in enforcing penalties for breaches of corporate policies. CS collaborates with the Marketing function as a source of technical expertise in sales pitches. This collaborative relationship is regarded as a supportive role as well as a control for protecting TELE-Co IP rights. CS also works closely with IT. The IT function provides CS with IT services. ISS secures remote connections with customers and collaborative partners. Teams such as the CMPR provide CS with a source of expertise in M-Gates. Additionally U.S Engineering is a source of support for the regional CS and Engineering teams dispersed across the TELE-Co subsidiaries.

ISS transparently supports every function and applies controls to both enable and restrict employee access to TELE-Co systems, repositories, forums and KM

tools. CS interoperates, as a technical advisor, with customer facing units to protect product designs and customer feedback.

It is from the above descriptions of the different units/functions within or interacting with the two functions that the following were identified: customer feedback, technical advisors, roles and responsibilities, coordinating group, and groups to enforce policies, secure connections, and escalations (Appendix F: Row 6).

(7.) Knowledge is also stored in **inter-organisational relationships**. The two functions avail of external knowledge in the form of collaborative partnerships. Vendors are used to collaborate in problem-solving and as a source of product specifications and standards. However the ISS function uses regulatory bodies as a source of externally approved standards and best practices. Auditors are used to review and evaluate ISS activities. The report generated, as a result, is used to plan and prepare for future reviews and for post-mortem brainstorming. IS forums are regarded as a source of knowledge. Forums consist of a network of ISS professionals from other multinationals collaborating and exchanging details regarding attacks or the customisation of best practices and standards.

CS uses knowledge collected from customers to alter product designs, the removal of flaws identified and the incorporation of potential trade-offs in product design. Conferences are also used by TELE-Co to determine the direction, for example, simulation software is taking and to play a part in leading new developments. Therefore the purpose of the TELE-Co symposia is to direct and collaborate with academia and industry. Public and government sponsored forums are also used as a source to estimate the future direction mobile technologies developments are taking and possible (environmental) restrictions that could be forced on the telecommunications industry.

The differences, regarding the inter-relationships used, are not profound. ISS exploits and attempts to direct regulatory bodies. In the process of doing so the function uses external evaluators and other organisations as sources of knowledge in order to comply and prefect ISS activities in terms of the environment the organisation is operating in. Similarly, CS makes use of customer feedback and conferences to manipulate the mobile market and incorporate identified customer requirements into product designs.

It is from the above descriptions of the different inter-organisational relationships that the following were identified: vendors: interoperability knowledge, regulatory bodies, evaluation groups, forums, specialist and public expertise, and government regulatory requirements (Appendix F: Row 7).

In summary the different levels of expertise are viewed as a significant source of knowledge within the two functions. CS created an ad hoc knowledge group and Coordinator to enable collaboration between the different design domains. Documentation from internal and external sources was used to comply with functional or corporate requirements, particularly in documenting lessons-learned and case solutions. Knowledge tools such as a central repository tool, vendor repositories and email are used to store knowledge. Finally it is evident that the functions are dependent on inter-relationships with an external evaluator for the ISS function and customer feedback for CS.

6.1.5.3 Functional Knowledge Processes

This sub-section summarises the different knowledge processes utilised by TELE-Co's IS Security and Customer Support functions. Appendix G is adapted from Tables 6.6 and 6.9. Knowledge is pulled from the ISS and CS reservoirs outlined in Appendix F and used through the processes outlined in Appendix G. The Table summarises, compares and highlights the differences between the processes used within the two functions. The third column illustrates the characteristics of the practices used to manage ISS and CS knowledge.

(1.) Knowledge **acquisition** is the process by which knowledge is obtained and internalised by TELE-Co. The IS Security function acquires regulation guidelines, and standards such as ISO17799. ISS methodologies are purchased, customised and used internally to suit the needs of the function. External expertise in the form of consultants are hired and used to evaluate the network boundaries, through testing, and internal controls for audit reviews

CS collaborates with and acquires knowledge from academics and other organisations through a yearly TELE-Co symposium. This platform enables the function to determine the direction of new simulation software and to direct the market. Reverse-engineering is a fundamental process in acquiring new knowledge. The technique allows the function to determine how competitors are building their products and if the improvements (if any) can be incorporated to enhance TELE-Co products. This knowledge is used in interoperability problem-solving as customers will inevitably be using other products in addition to the TELE-Co product portfolio.

The difference between the two functions approaches to sourcing external knowledge is their dependence on their individual external drivers. ISS is driven by the functions remit to comply with TELE-Co's environmental regulatory constraints. The function has to acquire necessary standards and best practices. CS needs to stay ahead of market developments and their competitors. Therefore, CS attempts to lead the market by facilitating a collaborative forum and reverse-engineer the competitions product offerings.

It is from the above description of the different acquisition processes that the following were identified: customised guidelines, methodologies and standards, industrial collaboration, reverse-engineering and external evaluation (Appendix G: Row 1).

(2.) Knowledge **capture** is the process of retrieving knowledge residing within practitioners, artefacts, and organisational entities. The two functions utilise a pool of experts to solve function related problems. Technologies such as a plethora of KM mechanisms are used to enable collaboration across dispersed subsidiaries. Email and the central repository Compass are the primary tools used to retrieve manuals, documentation and procedures. CS, in addition to the above, utilises simulation models to design and test data. Allocated roles and responsibilities are used in locating expertise and the escalation process enables practitioners and teams to pool expertise from different support levels within the organisation.

The only difference between the two functions in capturing knowledge is predominantly the simulation tools used by CS to retrieve product component

designs and the escalation process used. This has been due to the goals of the two functions. IS Security full-fills internal employee and function requirements and monitors the external network environment. CS builds and takes apart mobile products.

It is from the above description of the different processes for capturing knowledge that the following were identified: security technologies, simulation models: design and test data, roles and responsibilities, escalation processes, groupware and a central repository (Appendix G: Row 2).

(3.) Knowledge **creation** occurs when experts collaborate and use existing knowledge. IS Security and CS creates solutions through problem-solving processes. Lessons-learned are documented through the auditing process for ISS and in the utilisation of the M-Gates methodology by the two functions.

ISS utilises a trial and error approach in allocating controls in TELE-Co. Employees are granted access to different systems and documentation based on their roles and responsibilities within the organisation. However access rights change as employees require additional access or insufficient access was granted initially. This has been due an initial lack of understanding by the Finance department in enforcing segregation of duties for regulatory purposes. ISS have often reassessed access rights based on the feedback from employees and management. Lessons-learned and audit documentation are created and used to improve internal processes. Applying the M-Gates methodology or auditing steps result in the creation of lessons-learned documentation and review reports.

CS has undertaken a number of activities which have resulted in the creation of solutions and product builds. A divide-and-conquer approach is used to break a problem down into smaller parts to simplify the process, trouble-shooting guides and M-Gates are all used to solve problems and phase the development of TELE-Co products. Methodologies for product development and project management are used to coordinate a collaborative approach to problem-solving. Documents such as the SRD and risk assessment techniques are used to determine security requirements and identify security product enhancements.

However the CS function does not use an external evaluator to measure activities performed. CS utilises numerous KM mechanisms (such as M-Gates and brainstorming) to manage projects and to break down problems into more manageable chunks.

It is from the above description of the different processes for knowledge creation that the following were identified: problem-solving processes create solutions, trouble-shooting guides, M-Gates produces the following: product realisation, product development mile-stones, the auditing and escalation process, create a trial and error approach to granting access to knowledge assets, lessons-learned are created from reviews and planning. Finally security requirements are identified through M-Gates and risk analysis techniques (Appendix G: Row 3).

(4.) Knowledge **sharing** is the process through which explicit and tacit knowledge is communicated between individuals, groups, units or organisations. The two functions use the problem-solving process to create, store and share solutions. The solutions are often created through collaborating with other members of the

functions or in the case of CS with the customers themselves. However the IS Security function shares, through email, compass, teleconferences internally and utilises public forums, regulatory bodies and symposiums for external collaboration. ISS practices are shared externally to learn from and collaborate with other organisations in sharing lessons-learned and in steering the security industry.

CS share product designs, solutions and test data predominately internally. KM is used to share across the function not externally with partners. Therefore the difference between the functions in their approaches to sharing is that ISS will search for and collaborate with partners to steer the security market and CS will push or drive solution knowledge across the different design domains and CS teams.

It is from the above description of the different processes for sharing knowledge that the following were identified: the creation process is facilitated by email, Compass, teleconferencing. Problem-solving enables the creation of product designs, coding, trouble-shooting. Collaborative forums enable ISS to share issues with other security professionals working within different organisations as well as play a part in driving the security market (Appendix G: Row 4).

(5.) Knowledge **application** involves the use of knowledge in guiding decisions and actions. The ISS function utilised security technologies to build a picture of TELE-Co's security landscape. Standards and best practices were purchased customised and reused. Experts for knowledge trading and therefore problem-solving can be located through Compass. Audit reviews were used to improve ISS practices in the organisation as lessons-learned are documented. Email warnings from the TGS or external vendors use email to warn of potential threats so that Security Officers can avail of warnings and linked solutions to react to a potential problem.

The CS function utilises the M-Gates methodology to apply the knowledge generated at each gate. The outputs vary from the identification of project requirements, the allocations of necessary resources (such as a Security Advisor) to evaluate risks. Simulation software enables Customer Support to build prototypes and collaborate across the different design domains. However the software used cannot integrate the different product components created in each design domain. Experienced Engineers are used to integrate the designs manually. Reverse-engineering is also used to assess and incorporate competitor knowledge into TELE-Co products. Product builds, problem-solving are each enabled through collaboration and facilitated through email, teleconferences, and face-to-face meetings.

The application of knowledge in the two functions is very different. ISS purchases, customises and reuses external knowledge. Lessons-learned are documented through post-mortems and external measures or processes are used to improve internal activities and raise its political profile in the organisation as external audits have monetary implications. The CS function requires the use of a project management methodology to enable the coordinated reuse of knowledge. The function is also dependent on the tacit knowledge of its Engineers and their ability to innovate without the use of modelling software which at the moment cannot integrate the designs created across the different

design domains. As a result knowledge is pulled from different design domains and designers to innovate. ISS as a function purchases and customises external knowledge to predominately adhere to environmental requirements.

It is from the above description of the different processes for knowledge application that the following were identified: integrated view of the organisations security landscape generated from security technologies. Standards are purchased and customised for use. Audits have provided ISS with unexpected sources of knowledge. The review reports are used for post-mortems. CS utilises a standardised approach in managing projects but an innovative process to create new products (Appendix G: Row 5).

(6.) Knowledge **control** processes secure valuable corporate or functional knowledge. The IS Security function utilises a three pronged approach to control each facet of ISS. Security technologies are predominately used to control and protect knowledge. Systems are prioritised according to their value and the necessary recourses are aligned. Corporate resources such as HR repositories and Engineering labs are allocated controls in order to protect the innovative process and the innovators themselves. Controls are even allocated to documents to ensure consistency and ownership.

The CS function's access rights are domain specific. However Engineering has complete rights over their systems and labs so that the innovation process will not be interfered with. Virtual private networks are used to encrypt the communication lines between CS, Engineering and external partners. Legal documents, such as NDAs, are used to control employee behaviour. Penalties for breaking TELE-Co regulations regarding sharing IP with for example competitors are outlined and agreed through the NDA which is a formal contract.

It is from the above description of the different examples of knowledge control that the following were identified: Control Method, Alignment of Controls, Centralised Control, Testing of controls, Monitoring, Ownership /Decision-maker, Priority Systems, ACL /VPN/ Tunnelling, Legal and Control Documents (Appendix G: Row 6).

In summary a significant amount of ISS knowledge is acquired externally. Collaborative software, regulatory guidelines, subscriptions, technologies and external evaluations are acquired by the functions to ensure that the organisation is compliant with its business environment and aware of any and all business opportunities such as market changes and competitor products. Knowledge is retrieved from the reservoirs outlined in Appendix F and very much dependent on experts and knowledge tools. Problem-solving is the principal approach used to create knowledge and applied through the reuse of the solutions created.

6.1.6 IS Security and Customer Support KM Mechanisms

This section describes the **mechanisms** used in TELE-Co, either directly or indirectly, to promote the management of ISS and CS knowledge. Table 6.11 outlines the mechanisms which are divided by type, and illustrates which are common or unique to both functions and as a result available at an organisational level (√√). The first sub-section describes the mechanisms used at an organisational level, and the second at a functional level. Finally, this section concludes with an analysis of the mechanisms used.

(1.) Organisational Level

TELE-Co uses a variety of non-technological mechanisms to facilitate learning and enhance quality control in the organisation. As described by the Director of HR "a number of mechanisms are used: induction training for new hires to introduce them to our way of doing things. Specialised training is necessary for some organisations as there is a shortage of Software Engineers or graduates with special skills. We created TELE-Co University to up-skill our new hires". "Due to the special skill-sets required by TELE-Co in Software Engineering, Compliance and Customer Support we take in a lot of graduates as interns but we can never recruit enough [with the right skills]. We have created a TELE-Co University to deliver online training through E-learning and develop a wide range of core software engineering skills," as stated by the Director of HR. "Mentoring is a key process in TELE-Co it provides a new hire or an employee whose responsibility has changed access to an expert or a group of experts," as stated by the Former Project Manager. "Learning on the job, and manager – employee reviews are used to help employees learn and expand their skills here, reviews are a way to informally evaluate the employee and help guide their progress. We also use brainstorming sessions to develop profiles of our managers so that we know who we should make part of their teams," as stated by the Director of HR. As explained by the Former Engineering Manager "in a global organisation like TELE-Co teams are coordinated [primarily] through teleconferences, and when possible face-to-face meetings. Minutes of meetings are recorded and are TELE-Cos way of tracking projects and their status, usually these are then stored in Compass".

As explained by the [Cork] Security Officer "TELE-Co standardises everything [regarding] our jobs. Templates are used and tagged using a corporate format which [stipulates] the author [owner], date written, name of anyone who has updated or changed the document along with the reasons [for doing] and these dates. It's a way to manage our TELE-Co documents". "Project management [methodologies are] used to standardise the approaches across the multinational. M-Gates was developed in-house and it phases projects so that they are more manageable and require [specific] outputs like for example a requirements doc. Six Sigma is also used and practically a second language for TELE-Co employees in building a case for corporate resources," as explained by the Former Project Manager. Symposiums are used to "collaborate with Industry in driving certain goals of our organisation like the mobile market or for regulatory requirements," as stated by the Director of HR.

The central repository for TELE-Co is Compass. "It was created to allow TELE-Co employees to share information across the different subsidiaries. It is our Intranet, or a central document repository. Groups and communities of practice can collaborate through Compass as our Engineering teams or Security Officers are distributed throughout the globe," as stated by the Director of HR. As explained by the DB Analyst

"Compass has many functions which are available through four levels of access, as you [an employee] progress through the organisation you are granted more and more access to the different resources available through the system or it can be allocated based on your role and the group you are in". "Members can utilise a search tool and find experts or work-done on previous projects, it is as advanced as we need at the moment," as further explained by the DB Analyst. As described by the Director of HR "Compass is just a content management system (CMS); it is used to store documents and lessons-learned for the financial audits. TELE-Co University is the learning environment that we use to increase our employees skills. It identifies skills needed and provides either face-to-face training or online courses". "MS Outlook is the most used tool for communicating and sharing resources. Every group or function uses it to collaborate and share solutions either directly or indirectly by sending out warning emails from Engineering or TGS. If a bug or a virus has been identified emails with hyperlinks to internal or external solutions are distributed to specific divisions or the entire organisation," as explained by the [Cork] Security Officer. As explained by the CS Manager "Common shares are used by regional teams to store procedures and trouble-shooting guides, vendor portals are also vital for us as we need to have access to information about vendor products. A lot of the time we need to be able to reverse-engineer a competitor's product because the bug is due to an interoperability problem". Call logging systems are used "to track calls by employees and customers and log the different escalation levels," as explained by the Former Engineering Manager. "Two-way pagers from are issued to the majority of our Engineers and IT and Security organisations. They are used to provide twenty-four hour support and as a virtual connection to our scanning tools," as explained by the TGS Coordinator. Public portals are also used to [facilitate] collaboration with external programmers," as stated by Design Engineer 2.

(2) IS Security and Customer Support Function Levels

The IS Security and Customer Support functions use a number of knowledge mechanisms. Some tools are common, others are function specific. "Brainstorming sessions are used at [the] end of project phases [M-Gates] and audits [for compliance]," as stated by the [Cork] Security Officer. As explained by the TIP Coordinator, "conference calls are regularly arranged by the group especially during an audit". "On-the-job training through unofficial mentoring, job shadowing or employee rotation are used to speed up the learning process in the [security] group," as stated by the Director of HR. Employees are also motivated to "collaborate and mentor their colleagues with promotion schemes and monetary incentives," as stated by the Former Project Manager. As described by the TGS Coordinator "the overall [security] operation within the organisation is monitored by formal groups [TGS, in/external Audit Committees, and TIP] and on site [Security] Officers with review measures to determine the effectiveness of the procedures in place". According to the [Cork] Security Officer "new hires undergo an induction programme with security emphasising the security culture of the organisation. The new employees are made aware of all of the policies and the requirements to ensure that all of the corporate procedures are adhered to". "SETA is one of the best ways to educate employees of the risks to the company, it is [necessary] to remind them of threats like man-in-the-middle[22] attacks and TELE-Co ethics [for code of conduct], but these are useless if they are not enforced by HR [penalties for

[22] Man-in-the-middle attacks (MITM): is a form of active eavesdropping, through which the attacker makes independent connections with the employee(s) and relays messages from what seems to be a trusted source (for e.g. a bank) to obtain information such as a password. The information is then used to bypass ISS controls and sniff a corporate network.

breaking Security procedures]," as stated by the Security Coordinator. As described by the IT Manager "SRD require Security Advisors [depending on the project Security Officers or Engineers who specialise in Security enhancements] involvement in every stage of a project, they [Managers] must state the risks to TELE-Co and the Security controls, resources required for in-house or an external project".

The IS Security function depends on the different Security technologies to generate a picture of the TELE-Co Security landscape. According to the [Australian] Security Officer "we use a number of scanning tools to monitor our networks [subsidiaries] and identify anyone [rogues or employees] trying to access our systems or behaving in an unusual /unauthorised manner". Tools such as "VPNs for secure tunnelling with our partners and ART [Automated Analysis, Reporting Tracking Tool] feed us reports and identify vulnerabilities in our network, but the majority of controls are allocated to Engineering systems leaving other networks less secure and this is an obvious weakness yet controls / resources will not be as evenly allocated as we [Security] would like," as explained by the [Networks] Security Officer. "Excel and Outlook are our main tools for the job, Excel is used for creating risk matrixes, to calculate the levels of risk to critical systems so that enough controls can be added and email [is used] to check for any warnings from Microsoft, Cisco, McAfee or from TIPs," as stated by the [Cork] Security Officer. According to the Security Coordinator, "TELE-Co is an active member of regulatory bodies for developing [Security] standards and the International Security Forum to collaborate with leading companies regarding Security issues".

"Problem-solving or fire fighting is our [Customer Supports] job, we use email, a call tracking /logging system for escalations and Compass to collaborate with the different regional teams for our [product/component] division," as stated by the CS Manager. As described by the CS Engineer "trouble-shooting guides are very useful to us and we either develop them internally or we are provided with guides from our customers vendors. TELE-Co templates and guides are used for building solutions to errors or bugs identified by our customers, these are then stored in Compass or in our regional shares". According to the CS Manager "CS collaborates a lot with Marketing, we act as Technical Advisors to shadow a Marketing Manager during a sales pitch with a customer, we are their product experts and we know what should or shouldn't be said to a customer about our new products".

As explained by Design Engineer 3 "[the] M-Gates methodology is a phased approach to [not only] managing projects [but to] sharing knowledge across the different teams or [Design] domains. The CMPR [Concept to Manufacturing Process Redesign] team developed it and are the official experts on the methodology if [you] have any questions they provide excellent help". [The] "PKM team were unofficially formed by Design Engineers to encourage collaboration across the different domains to [ultimately] reduce the time involved in designing a product and handing it over to Product Developers. PKM is coordinated by the Knowledge Champion of the team", as stated by Design Engineer 2. According to the PKM Coordinator, "prototyping is our approach to testing new designs and building alternatives, using our modelling software, we store prototypes and test data, even if they are not used as we can quickly eliminate problems encountered in future releases or designs". "Our modelling software and lab simulations allow us to experiment, to innovate and create new products, simulations are brilliant learning environments in creating and problem-solving for customer problems and new requirements," as further explained by Design Engineer 1. Additionally, according to the PKM Coordinator, "TELE-Co Symposiums are organised by the company to

collaborate with academia and industry to determine the direction in simulation [software] or compliance [practices]".

Customer Support uses a number or tools to collaborate across and within the various functions. As stated by the PKM Coordinator "simulation models and software [system and paper-based] for product component designs are vital to test and share ideas. They give a 3D representation of an Engineer's ideas and allow us to collaborate, to be innovative". "CAD [computer aided design] tools are used to help us design our products, [and] we can also store the designs," as stated by Design Engineer 2. However the "simulation software used cannot facilitate the combination of all of the different Design Domains and we could be working on multiple components but this is where our experienced Engineers can pull everything together to form the integrated prototype before it's passed on to Product Developers. M-Gates and PKM force a more collaborate design initiative and phase the design [process]," as stated by the PKM Coordinator. Additionally according to the Director of HR "every effort is made to make these [Engineers] as productive and as innovative as possible, they have full control over their Labs [and networks], and use the latest simulation modelling software and we use brainstorming sessions to build profiles of our key Engineers. A HR database is used to create and record profiles of Engineers and match-up their teams". The organisation also utilises an online forum to collaborate with the general public "on programming queries so that we can promote ourselves to third-level student," as explained by the Director of HR.

The next sub-section compares KM mechanism usage by the ISS and CS functions.

(3) TELE-Co KM Mechanisms

Table 6.11 outlines and summarises the different KM mechanisms within TELE-Co which were verified by the Knowledge Consultant and the [Cork] Security Officer. The mechanisms are supported by the organisational infrastructure (section 6.1.2). Forty-six KM mechanisms were identified. The proportion of mechanism usage within the two functions was high with seventy-one (ISS) and seventy-eight percent of the mechanisms available used. Overall fifty percent of the mechanisms identified were categorised as organisational (used by the two functions). Thirty percent of the organisational mechanisms were identified as non-technological and nineteen percent as technological. Learning mechanisms, mentoring, induction training, face-to-face meetings, brainstorming sessions, quality reviews and the documentation of lessons-learned, groupware, symposiums and the corporate Intranet were each exploited by the ISS and CS functions. The contribution of IS and CS practitioners to TELE-Co was reported to be easier when knowledge was made accessible through the M-Gates methodology and Compass. The content stored was explicit, shared and modified if required. TELE-Co combined its document management system with Compass to provide centralised knowledge. The other mechanisms used by the two functions were identified as: common shares, technological forums, vendor portals, Excel, email, TELE-Co University, electronic contact lists, internal repositories, expert list, hyperlinks and two-way pagers. The mechanisms used to facilitate socialisation included: cooperative projects across the functions (M-Gates) and external forums.

Combination was facilitated by collaborating through documentation management systems (DMS), problem-solving, escalation processes and web-based access to knowledge. The integration of Design knowledge was regarded as a strategic initiative. The PKM group was established to combine explicit and tacit knowledge of Design

Engineers. Simulated software was used by Engineering to design new products and aid decision-making in determining the most appropriate design. The combination of the group and software was to encourage collaboration across the different design domains. However, this initiative is very much domain specific as opposed to functional and organisational. CS utilised Compass – a central repository, portals and group shares to store, retrieve and use functional knowledge. Knowledge sharing was enabled through the use of repositories, portals, expertise locators and the corporate Intranet – Compass. Knowledge application is dependent on the hierarchical relationships outlined in the structure of the organisation. The escalation process was identified as a key mechanism for sharing and using solutions which were often created using email. Thirty percent of the CS mechanisms identified were categorised as non-technological with forty-seven percent as technological. These high percentages indicated a significant difference in its use of non-technological mechanisms such as mentoring, ad hoc groups, roles and simulation models. CS utilised an ad hoc group and a Knowledge Champion to promote and drive KM across the design domains. Forty-one percent of the ISS mechanisms identified were categorised as non-technological with thirty percent as technological. The ISS function utilised non-technological mechanisms such as SETA to control employee behaviour regarding external risks and threats to TELE-Co. Formal groupings were established to drive the different facets of ISS. The TGS and TIPs groups were established to source regulatory standards, coordinate internal security and perform internal audits. Additionally participation in regulatory bodies and ISS forums enabled the organisation to steer the ISS regulatory market. Security technologies were used to scan the geographically displaced subsidiaries to develop a picture of the TELE-Co security landscape. ISS knowledge was also captured through solution templates and stored in repositories and accessed through where it can be easily retrieved by ISS practitioners.

Table 6.11 illustrates the high volume of KM mechanisms used in TELE-Co. It is evident that ISS utilised formalised mechanisms and external measures compared to Customer Supports ad hoc mechanisms to drive KM within the function. The significant difference between the functions was the more formalised approach to promoting ISS knowledge management than CS knowledge. CS positioned its KM initiative around M-Gates and PKM for specific design domains as opposed to the function. ISS utilised KM mechanisms to supports the functions goal of protecting the corporate assets and adhere to regulatory constraints. However the utilisation of simulation models could aid the ISS function in adopting a more proactive approach to supporting the security needs of TELE-Co.

IS SECURITY AND CUSTOMER SUPPORT KNOWLEDGE MECHANISMS				
	Mechanisms:	**Use:**	**ISS**	**CS**
Non Technological	Induction Training:	Specialised for the different functions & as an introduction	√	√
	Learning on the Job:	Responsibilities are added gradually	√	√
	Lab Simulations:	Learning environment to create new products & experiment		√
	SETA:	Penalties for Breaking Security Procedures	√	
	Mentoring:	Provide Access to Experts & a Ready-made Network	√	√
	Teleconferences:	Used for Global Communication	√	√
	Reviews:	6 month Assessment of Employees	√	√
	Minutes of Meetings	Recorded & Stored in Compass	√	√
	Face-to-Face Meetings:	Yearly Meetings (attempted, constrained by budget & time)	√	√
	TELE-Co University:	Up-skill to meet Specific Needs (not inc. in 3rd Level Courses)	√	√
	Brain Storming	Audit Reviews of Engineering Domains through M-Gates	√	√
	Expert Status:	Expertise List	√	√
	Quality Doc. Review	Internal Document Sign-off Procedure (Author Tracking)	√	√
	Technical Advisors:	CS Collaborate with Marketing to Shadow a Sales Pitch		√
	Symposia :	Collaborate with Industry in Driving the (Regulatory) Market	√	√
	DMS:	Doc. Templates & Quality Procedures (Authors/Editors/Dates)	√	√
	Problem-solving Process:	Escalation Process		√
	SRD:	Aligning Security Requirements to a Function Project	√	
	Six Sigma:	Build a Case for Project Resources & ID Responsibilities	√	√
	M-Gates: Methodology	Phased Approach to managing projects		√
	Trouble-shooting Guides:	Templates & Guides for Building Solutions		√
	External Evaluation:	Auditors (Review) & Security Vendors (Penetration Testing)	√	
	TGS:	TELE-Co Global Security Group: Coordinate Teams	√	
	TIP:	TELE-Co Intellectual Property Global Compliance Group	√	
	PKM (Ad hoc)	Team to encourage collaboration across Engineering Domains		√
	CMPR Team:	Concept to Manufacturing Process Redesign, M-Gates Experts		√
	Knowledge Coordinator	Champions KM Approach to Virtual Prototyping		√
KM Technologies	Compass: Intranet	Central Document Repository, Group Resource, Contact Lists	√	√
	MS Outlook:	Collaborating & Sharing Solutions	√	√
	CMS:	Stores Lessons-learned, Document Store	√	√
	MS Excel:	Risk Matrixes, to calculate the level of risk	√	
	Emails: In/External	Warning Alerts	√	
	Emails: Internal	Solutions & Hyperlinks to Guides		√
	Hyperlinks	Links to Internal & External Solutions	√	√
	Common Shares	Groups, Regional Shares, Stores Procedures and Guides	√	√
	Vendor Portals	Procedures, Guidelines and Best Practices	√	√
	Simulation Models	System & Paper-based for Product Components		√
	CAD Tools:	Computer Aided Design for Product Simulations and Stores		√
	Call logging System	Calls are Tagged by Expert & Escalation Levels	√	√
	ART:	Automated Analysis, Reporting Tracking Tool	√	
	Scanning SW:	Monitors Rogues & Internal Employees	√	
	VPN:	Tunnelling to Protect NW – Partners & Customers	√	
	Security Forum:	International Security Forum	√	
	TELE-Co Forum:	Public Programming Q&A Forum		√
	HR Database:	Records Profiles of Engineers & Used to match-up Teams		HR√
	Wireless Technology:	2-way Pagers from Systems or Call logging System	√	√
***Organisational Level: √ ISS** and **√ CS** *** Specific to One Function:** √				

Table 6.11: TELE-Co KM Mechanisms.

6.1.7 Impact of Managing IS Security and CS Knowledge

This section describes the impact of managing IS Security and CS knowledge within TELE-Co. The direct and indirect management of this knowledge has impacted the organisation at the following three levels: (1) individual; (2) functional and (3) finally at an organisational level.

Level (1) Individual Impact

The rate an employee climbs the learning curve "depends heavily on what resources his/her individual manager provides, rather than on the [collective] body of knowledge available in TELE-Co," as stated by the Director of HR. TELE-Co University provides "essential training for employees in general regarding security issues and TELE-Co intellectual property guidelines", as explained by the [Cork] Security Officer. As stated by the TGS Coordinator "security technologies and external sources like Microsoft [Vendors] provide us with a lot of knowledge about the network as well as potential risks". ISS practitioners are encouraged to "attend security conferences and forums such as [the] ISF [Irish/International Security Forums], to talk to other [Security] coordinators and share experiences and best practices", as explained by the Security Coordinator. According to the [Australian] Security Officer "we really depend on the different tools used in TELE-Co so that we can work together and solve problems as well as follow corporate guidelines [regarding] rollouts and SOX". According to the TGS Coordinator "all of the sites and GEOs are assigned to individual Security Officers and Coordinators so that the correct controls are provided for each TELE-Co manufacturing plant or R&D centre". Structurally ISS is a separate function from IT in TELE-Co. "Having a separate function [from IT] allows a separate budget and much needed political support [all of which is] due to SOX and 9/11", as explained by the TIPs Coordinator.

"KM tools and systems have enhanced TELE-Co's ability to create knowledge, capture it in a usable format, and reuse it for different projects," as stated by Design Engineer 3. "PKM processes build intellectual capital by facilitating learning and communities of practice," as stated by the PKM Coordinator. "[KM] tools help retain the results of our [functions] learning and make Engineering expertise available around-the-clock, world-wide. By using structured, standard processes it is possible to build global teams," as stated by Design Engineer 2. Furthermore, "employees seem to enjoy their work and can grow in their careers at TELE-Co, as PKM processes and tools help create a more stable environment with readily available design knowledge," as stated by the Former Engineering Manager. Tools are essential to "provide access to past [product] designs and solutions and we need to experiment with simulation software and processes like prototyping and PKM", as explained by the Former Engineering Manager. However "it is the TELE-Co University and Symposiums that provide the necessary skills for our [Design] Engineers and support Engineer as well as allow TELE-Co to steer the industry", as stated by Design Engineer 1.

Level (2) Function Impact

Specialised ISS (TGS & TIP) groups coordinate and share knowledge across the organisation. As explained by the TGS Coordinator "[the] security [function] is separate from IT and focuses on the different aspects of security. We use a three-pronged approach to ensure that the technical side of security is managed as well as monitoring and protecting TELE-Co assets for the organisation as a whole. We also have a group

that specialises [in] auditing to make sure we are all [subsidiaries and GEOs] compliant as the implications of not being are pretty severe". "Auditing is time intensive but we learn from each cycle and [reviews] are used to see if we are doing what we are suppose to be doing by corporate as well as the [external] auditor", as stated by the [Australian] Security Officer. "We do collaborate but it's mostly due to the different audits, we have to [adhere] to TIPs requirements. Obviously, to stay ahead of hackers, the groups share knowledge and resources across the GEOs through Compass and from our vendors", as stated by the Security Coordinator. As explained by the TIP Coordinator "audits have resulted in the documentation of everything including lessons-learned for our brainstorming sessions. They have forced a more practical approach to using or forcing what we have learned from one audit to the next and for our incident teams in targeting hackers or internal risks like an unhappy employee". ISS also use a "trial and error approach for figuring out how many controls or how restrictive we should be as we don't want affect productivity in TELE-Co – it's just a constant battle to protect TELE-Co assets and make sure groups like Engineering can access what they need", as explained by the Compliance Coordinator.

PKM processes and tools help to manage the "down side" of a project or design. The data-centric process of prototyping "enables designers and product managers to understand parameters impacting risk", as explained by the PKM Coordinator. As stated by the Design Engineer 1 "based on best-in-class design domain knowledge and a characterisation of design trade-offs, it is possible to identify and quantify the likelihood and impact of risk [events] such as the project being over budget, the product design process taking longer than the allocated time, the design being more expensive than the target cost". PKM provides a method for assessing the predictability of schedules, processes, and product requirements. Standardised documents and templates "ensure easy collaboration for problem-solving and advanced filtering for solution [Compass] searches", as stated by the DB Analyst. According to the PKM Coordinator "prototyping tools, and knowledge management as well as M-Gates allow us [Design Engineers] to collaborate as communities of practice when designing different [product] components and figuring out how the parts fit together". "Greater collaboration would reduce the inefficiencies of using different design domains, but it's really up to senior management to agree to using something like PKM across WEC", as explained by the Former Engineering Manager.

(2.1) Product / Service Impact

As explained by the Security Coordinator "best practices and standards are selected from vendors and regulatory bodies so that we use the best [approaches] and we follow industry standards". "Auditing is now very useful and they do provide a lot of information or knowledge about how good we are at securing TELE-Co. We do make every attempt to sit down or organise teleconferences at the end of each one so that all [of the] lessons-learned are recorded", as stated by the TIP Coordinator.

"Reverse-engineering provides very useful knowledge about the different product our customers are using. We need to know how these products work so that we can solve inter-operability problems and obviously to [determine] how good our competitors products are", as explained by Design Engineer 2. According to the Former Engineering Manager "first to market is every Engineering organisations goal [in order] to maximise profits and reverse-engineering is a skill or technique used to achieve this". "We use a lot of things to enhance the service we provide. Our support engineers need to have diagnostic skills and know who to escalate problems to as well as the right trouble-

shooting manuals and solutions [to] support customers and [as a result] our products", as stated by the CS Engineer. Collaborating with Marketing as a technical advisors "allow CS and Engineering to collect important customer feedback [regarding] trade-offs and fixes", as explained by the CS Manager. As stated by the PKM Coordinator "sharing knowledge across the different design domains will reduce design and development times. We just need more and more Engineers to participate and then management will adopt PKM throughout TELE-Co like M-Gates".

(2.2) Processes

ISS utilises "a number of tools like POPI to ensure the functions effectiveness in securing TELE-Co", as stated by the [Cork] Security Officer. "Brainstorming sessions at the end of each review are pretty common. They are difficult to organise because of time differences as well as finding the time needed to chat, email and record the lessons-learned", as stated by the [Australian] Security Officer. As explained by the TGS Coordinator "we use Compass, vendor sites, ISF, TELE-Co processes like M-Gates, standards and the best practices selected by TIPs". According to the Compliance Coordinator "reviews are used to guide future audits, document the different processes and as a form of assessment for [the] security [function]

Effective decision-making has an indirect impact on an organisation. As explained by the PKM Coordinator, decision-making is defined as, "an individual or group process that takes knowledge about a given scenario, and selects one or more potential courses of action". Decision-making in TELE-Co includes the following: "identifying the decision stakeholders and their roles in the decision-making process, selecting criteria based on which the decision is made, gathering information, identifying and evaluating [alternatives], and selecting the best [alternatives]," as stated by Design Engineer 2. As described by the PKM Coordinator "the effectiveness of a decision-making process can be measured by the time needed to make decisions, how well they [timeliness of decisions] match scheduled times when action is required, how well they [robustness of decisions] account for uncertainties and risks, cost or effort of the decision-making process, how well the decision-making process is understood and visible throughout WEC [the Engineering organisation] or other organisations [functions]". The validity of the decision-making process, that is, "how well it follows generally accepted principles, the clarity of the decision alternatives selected by the process, and the acceptance of the decisions from the process or TELE-Co buy-in," as stated by the Former Engineering Manager.

As explained by Design Engineer 2 "the primary way in which the impact of PKM can be measured is cycle time the time required to transform a concept into a production product". Cycle time can also be measured for each of the individual process steps or stage gates within the product realisation processes. "Cycle time is measured [according to] the time to complete a given process step, [for example a prototype], and the number of steps to complete the total process," as explained by Design Engineer 2. According to the PKM Coordinator "the goal of PKM is to create a process with fewer and faster prototype cycles". Access to reliable and timely knowledge is crucial for cycle time reduction. "If knowledge is not reliable, a [Engineering] Designer or Project Manager making decisions will make errors. These errors can [subsequently] multiply as decisions are made using the wrong results of the original decisions. At best, this will result in the need for error correction activities if the error is detected. At worst, the error will not be detected until the product reaches the market," as explained by the Former Engineering Manager. "The time spent on [error correction and] damage control

would be actually better spent executing the product development process," as further explained by the PKM Coordinator. "Standardised templates allow us to incorporate fairly advanced searches for Customer Support and we do try to monitor solution use through Compass but it is just a repository and not a tracking case-based reasoning tool", as explained by the DB Analyst. As stated by the Former Engineering Manager "internal processes and approaches like M-Gates as well as Six Sigma are developed internally. TELE-Co uses internal expertise and rarely looks externally unless it's to reverse-engineer a product. Even internally it's difficult to work across the different design domains. TELE-Co is very much dependent on Engineering expertise in combining different designs and figuring out trade-offs". "PKM is the solution for our Engineers to share and understand the different risks", as stated by the PKM Coordinator.

Level (3) Organisational Impact

The impact of ISS is difficult to measure. "A cost model is used in TELE-Co manufacturing sites to determine the downtime for production and the overtime needed to fix a problem resulting from a security breach", as explained by the Security Coordinator. As described by the TGS Coordinator "obviously a low level of security will have a dramatic affect on the image of an organisation if, for example, a breach in TELE-Co was made public – customer confidence in our products would be reduced". "Like every organisation we have experienced [security] incidents and can calculate the cost in downtime and in the resources needed to fix things but really it's a work-in-progress in trying to come up with a ROI type measurement", as stated by the [Networks] Security Officer. "Audits are measures of how we apply controls and [determine] access rights for TELE-Co employees. It's also a trial-and-error kind of approach [because] we are always updating peoples access so that they have what they need to do their jobs", as stated by the [Cork] Security Officer. According to the Compliance Officer "compliance and 9/11 changed managements [and] everyone's idea of security, there are financial implications if TELE-Co isn't compliant, our customers expect us to be and we know that to make things easier for ourselves - we have become active members of [security] regulatory bodies to drive the market and play a part in agreeing new standards and practices". IS Security is directly aligned to the organisations strategy as "we regularly check to make sure that security is mapped to TELE-Co processes and the [security] policy is mapped to the goal of the organisation", as stated by the Security Coordinator.

CS and Engineering costs are incurred if "delivery of a product is pulled as fines are demanded by the customer", as stated by the CS Engineer. The cycle time benefits are closely related to the risk mitigation benefits of PKM. If the flow of knowledge at a given "step in the product realisation process is not timely, it will [in most cases] delay the execution of subsequent steps", as explained by Design Engineer 1. When it is necessary to move forward to the next step in the project schedule, "[the] Project Manager may opt to do so with incomplete knowledge, [thereby] increasing the risk associated with the design", as explained by the Former Engineering Manager. Risk is introduced into the project/product by the lack of knowledge to support a timely, high-quality decision. As stated by the CS Engineer "the PKM team believes that if reliable and timely knowledge flows were available within TELE-Co's product realisation process, dramatic reductions could be achieved in both product cycle time and project risk". Cycle time improvement is an organisational goal. It is "the main lever for driving cost reduction," as stated by Design Engineer 2, which is the primary area in which the benefits of PKM can be measured. Increasing the productivity of Designers and

therefore reducing "the level of effort for a project will reduce Engineering costs", as stated by the CS Manager. As described by the PKM Coordinator "total Engineering costs are roughly proportional to the number of prototype cycles that need to be completed for a given product". Based on the analyses by the CMPR team in the first quarter of 2001 [TELE-Co website], it was determined that "even a five percent improvement in Engineering costs [through the application of design simulation and prototyping] would lead to a significant reduction in the overall Engineering costs for a new product", as stated by the PKM Coordinator. "The PKM team developed an activity-based cost (ABC) model, that incorporates the staffing levels and cycle times for each of the gate owners and suppliers for the M-Gates methodology," as stated by the Former Engineering Manager. As explained by the PKM Coordinator "the financial impact of PKM is generally viewed in terms of reduced Engineering costs, due to fewer prototype cycles, faster prototype cycles, and a higher level of design reuse and knowledge sharing". "It is possible to generate increased revenue, thanks to better satisfaction of identified customer requirements, higher quality products, more customer-centric designs, and earlier market release," as further explained by Design Engineer 2. Finally "the return on investment [ROI] for project management activities has been pigeonholed in terms of organisational maturity, project schedule slippage, and budget slippage. If we can reduce these the overall benefit will be huge," as explained by the CS Manager.

6.1.8 Summary: Managing ISS and CS Functional Knowledge

The TELE-Co findings also provided rich descriptions of the approaches used by the two functions in managing knowledge. Table 6.12 outlines and summarises the different impacts generated as a result of the approaches used to manage knowledge within the two functions. While CS utilised a KM approach to prototyping, the IS Security function benefited from formalised processes used to manage the organisations regulatory requirements. The IS Security strategy was aligned to business strategy. Non compliance has financial implications and provides the function with a measurement. Membership of regulatory bodies was and is a necessity as it allowed TELE-Co to participate in driving the industry. However KM was not aligned to business strategy. KM was implemented on an ad hoc basis and specific to CS and Design Domains. Therefore ISS is more effective in managing knowledge than the CS function. However the utilisation of simulated software for incident decision-making could allow the function to document rogue behaviour and predict and plan for future incidents. The impact of the regulatory and internal control mechanism are analysed in Chapter 7 in leveraging IS Security on a KM environment in order to address the third research question. The analyses necessary to address the three research questions will also enable the researcher to derive a model for managing IS Security knowledge.

IMPACTS		ISS FUNCTION: NO KM INITIATIVE	CS FUNCTION: KM INITIATIVE
(1) Individual \s	Learning	Access to SETA programmes through the Corporate University.| Security conferences, Employee reviews as well as external reviews.|	Prototyping & KM facilitate learning for Design Engineers. University develops core skills. Attendance of Engineering conferences & TELE-Co Symposia for collaboration.
	Adaptability	Security Technologies & Threat complexity is high & constant, Knowledge Tools: centralises knowledge.| ISS Expertise coordinated.	KM Tools (such as Compass) retain individual knowledge for reuse.| Available design & solution knowledge reduces the time needed to solve a problem /design a new product.
	Satisfaction	Job is easier due to specific processes & tools/practices available.| Political support at senior level.| ISS technologies provide knowledge.	Access to greater number of solutions (Compass): reduces the complexity of problem-solving. Simulation SW provides access to past designs.| Knowledge is centralised.
	Adaptability	Specialised (TGS & TIP) groups coordinate & share knowledge across organisation.| Audits provide a measures & learning.|	Development standards (M-Gates|PKM) & Templates ensures easy collaboration & advanced filtering for solution searches.
	Satisfaction	Shared knowledge across the different groups.| Proactive stance against risks through brain-storming, lessons-learned.|	Collaborative teams are possible through structured development processes. However, SW designs are specific to design domains which can be frustrating.| Access to CoP.
(2.1) Product /Service	Value-added	Best practices & standards are sought & evaluated to improve security within the organisation.|	Reverse-engineering & diagnosing skills provide valuable knowledge re: competitor and customer products/problems.| Escalation processes enables improved service & products for customers. DMS enables the creation of detailed solutions.|
	Knowledge (based)	Fewer surprises in regular audits & increased security information.| Lessons-learned from Audit post-mortems.	Improvements on products from Customer feedback & repeated bugs are passed back to Engineering to fix in the next release. Faster response time for fixes.| Pushing knowledge around the design domains reduces time needed.| Experienced Engineers combine designs.|
			Solutions for problems/designs are not made available to Customers or to some Domains.
(2.2) Processes	Effectiveness	Brainstorming sessions.| Use of GW (email) & repositories of Best Practices, Standards, & lessons-learned.| M-Gates, SRD, & POPI	Employees are mentored by Engineers.| Use of Prototyping, KM to integrate and leverage design knowledge.|
		Reviews are used to guide the next review.| Ongoing evaluations	Fewer mistakes made.| Time to Market reduced.|
	Efficiency	High number of external sources.| High volume of K stored in repositories, technologies.| Number & use of ISF Forums.| M-Gates is used as a best practice approach.|	No. of Solution hits is monitored.| Reuse of Solutions through Compass.| M-Gates is used as a best practice approach.| PKM enables Engineers to understand parameters impacting risk (of failure/over budget).| Method for understanding schedules & product requirements.
		No. of improvements as a result of an Evaluation.| Auditing requires the documentation of ISS processes.	Low number of external web sources used; High volume of Knowledge stored in repositories.|
		Audit process- enables learning, measurements, post-mortems & guide next review.|	A CBR Tool is not used to enhance & support problem-solving.| DMS & Compass: centralise & standardise.
	Innovation	Brainstorming for Audit reviews to improve the process & the evaluation.	Engineers combine the design knowledge created from single domains & simulation SW.| Trade-off knowledge is captured & incorporated into designs. | PKM enables integration.
(3) Organisation	Direct	Security strategy is aligned to business strategy.| Non compliance has financial implications.	KM is not aligned to business strategy.|KM is ad hoc & specific to CS & Design Domains.| No support from Senior management in PKM adoption.| First to market- new products
		Difficult to measure ISS – downtime & overtime necessary to rectify an ISS breach can be calculated.	Reduction in escalations reduces costs.| Learning & design times are reduced.| Reduction in cycle-times.| Monetary penalties are incurred if a product is late (ABC).
	Indirect	Poor security has dramatic affect on Corporate image.| Auditing allows an unbiased measurement of the function.	Collaboration across Domains to ultimately improve the process & the realisation of first to market.| CS collects and incorporates customer feedback.| Effective decision-making.
		Best practices are shared.| Membership of regulatory bodies to drive the industry. An overly restrictive environment	Best practices are shared across participating Design Domains.| Symposiums drive market.

Table 6.12: IS Security and Customer Support Impacts.

CHAPTER SEVEN

INTERPRETING HOW ISS CAN LEVERAGE THE CONCEPT OF KM

7.0 Introduction

This Chapter analyses the findings to address the research questions by using a cross-case analysis. The Chapter consists of three primary sections (sections 7.1; 7.2; 7.3), one for each of the research questions. The following sections highlight the findings associated with each component of the research framework (Figure 7.1) identified from the synthesised IS Security and KM literatures discussed in Chapter two (Figure 2.5) and set out in Chapter 3 (Figure 3.1). The framework was used as a lens to analyse the different operational factors and outcomes identified in literature and to differentiate between them through their applications within CME-Co (Chapter five) and TELE-Co (Chapter six). The factors and outcomes acted as a basis for grounding the investigation of the approaches used to manage knowledge in two specialised support (IS Security and CS) functions. Chapters five and six examined how the two functions managed knowledge within the organisation.

This Chapter discusses how KM can be leveraged to manage IS Security knowledge across the two organisations. Section 7.1 discusses how the different components of the organisational infrastructure can support the management of IS Security knowledge. Section 7.2 describes the concept of managing IS Security knowledge. The intention is to understand how organisations manage this knowledge. Section 7.3 discusses how firms align IS Security to a KM environment. 7.4 describes and justifies the model derived from this analysis. Each section of the four sections brings together some of the key issues identified in the two case organisations, and draws out some general statement for interpreting the management of IS Security knowledge. Finally, section 7.5 concludes the Chapter.

7.1 Organisational Infrastructure Supporting the Management of IS Security Knowledge

This section discusses the concept of organisational infrastructure. The intention is not to undertake a review of the literature, but to understand how the organisational infrastructure can support the management of IS Security knowledge and therefore protect the organisation and its processes. The following sub-sections highlight some of the basic ideas associated with each organisational infrastructure component. Section 7.1.2 describes the common knowledge utilised. Sections 7.1.3 and 7.1.4 respectively explain the importance of the corporate physical environment and structural requirements for ISS. Sections 7.1.5 and 7.1.6 describe the IT infrastructure necessary and the importance of the business environment in which the two case organisations operate in. The first part of each section interprets the components in the two organisations. The second compares each to literature. Finally, a synthesised perspective on how the organisational infrastructure can support the management of IS Security knowledge is presented in sub-section 7.1.7. However, first cultural dynamics are discussed.

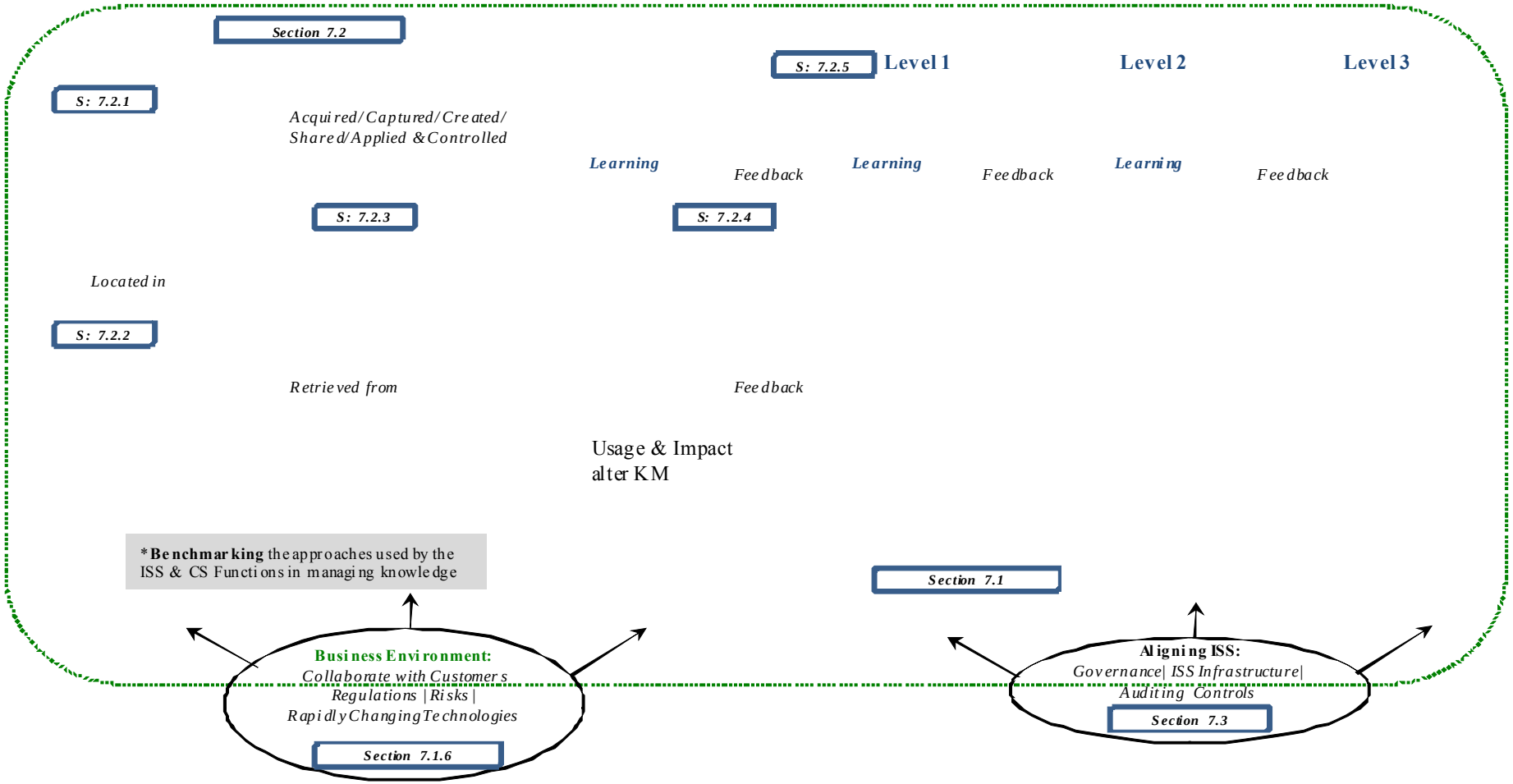

Figure 7.1: Conceptual Model (Figure 2.5): KM Approach to the Management of IS Security Knowledge.

7.1.1 Interpreting IS Security Cultural Dynamics in the Case Studies

The CME-Co and the TELE-Co multinationals displayed a consistent effort to promote a culture of knowledge sharing. However, in both cases it has and continues to be a battle to prove to employees that they will benefit from being more open (Hislop, 2005). Significant blame can be attributed to the manner in which management of the two organisations view KM. It was evident from the two the case organisations that KM has been relegated to the form of an IT solution rather than with the organisational culture and with the employee incentive reward structure used by the two case organisations. TELE-Co and CME-Co have, at a corporate level, implemented a global content management system (CMS) as their solution to a KM initiative. This was in spite of the vocal demands by academics and practitioners alike that KM and a culture of knowledge sharing should be supported at the senior levels in an organisation. KM needs to be considered as a strategic issue, especially in today's climate where it was becoming difficult to compete and internal resources should be utilised more effectively.

Mechanisms such as mentoring, SETA and employee rotation are used to encourage employees to share knowledge. Analogies are used to develop cultures of competition in both cases which has been reported as effective by interviewees. CME-Co strives to encourage this ethos of business daring and pride in its successes. Employees are encouraged to be regarded internally as gurus in their areas of expertise. However knowledge sharing in the cases was function or team specific. The Customer Support function in CME-Co regularly battles senior management, and particularly Engineering, to share internal knowledge. The PKM community of practice, despite the obvious benefits of sharing designs across the different (design) domains, continuously tries to prove the financial benefit of sharing to TELE-Co senior management. Therefore specific functions have knowledge sharing cultures, and attempt to allocate time and resources to enable staff to share. CS drives KM in both cases as it was a fundamental aspect of their role in the organisations. The day-to-day activities the CS functions described in the case organisations was problem-solving and the more they share knowledge the faster and cheaper the process. However, Engineering units are reluctant to share product designs, specific commands and bugs due to the financial risks of this knowledge becoming public. It was through the sheer persuasiveness of the CME-Co Knowledge Champions in proving the cost-saving benefits of pushing knowledge towards the customer that the culture was becoming more open. The geographical spread of the organisations was also an obstacle to a culture of sharing and control. Managing different cultures is difficult when language and even time zones are factors. Building relationships through face-to-face (F2F) meetings has been identified as the best approach to combating these problems and the two case organisations have encouraged this.

Changes in the business environment created a culture of security awareness for the two case organisations. Senior management were committed to enhancing security both internally and externally so much so that it became an inherent part of organisational operations. Traditionally security was categorised as an IT problem. Since 9/11 and regulatory changes such as SOX, ISS has become one of the key business drivers for CME-Co and TELE-Co. The two case studies identified the possible competitive advantage that can be gained from incorporating security enhancements into their products, steering standard making bodies and providing a one-stop-shop for customer compliancy requirements. As a result roles and official groups have been established in the two cases raising the profile and political power of the IS Security functions. The

resources necessary to enable the global function to collaborate were also allocated. However the circumvention of (security) controls by Engineering continues to create a culture of resentment from a security perspective as it weakens the control environment used to protect organisational assets. Therefore from a IS Security and CS (front-line support) perspective a culture of entitlement and circumvention of rules creates knowledge sharing issues for both functions despite the fact that security was aligned strategically to the goals of the two case organisations. Consequently, managing IS Security knowledge was vital in order for IS Security professionals to be proactive regarding security - particularly in sharing (SETA) threat and risk knowledge with the general employee population.

7.1.1.1 IS Security Cultural Dynamics

The two case organisations fostered very competitive cultures (Tsohou et al., 2006). The corporate ethos was ingrained into employees, initially through the two corporate universities, then through norms and practices, corporate symbols, and in-house Engineering terminologies (De Long & Fahey, 2000; Pettigrew, 1979). CME-Co assigned individuals (particularly Engineers) with hero statuses to promote knowledge sharing (Davenport & Prusak 1998; Walsham 2001). Stories of living CME-Co legends and their business daring that epitomised the corporate philosophies of: the customer is always right and minutes equals millions were common. The targeting of competitors in setting corporate wide goals not only facilitated a corporate level culture of competitiveness but also at functional and subsidiary level as geographies and functions competed to meet targets.

The two organisations exhibited strong functional cultures (Deal & Kennedy 1982). The Customer Support functions developed internal strategies to cope with diagnosing and solving problems (Schein, 1985). The problem-solving escalation procedures utilised were evident within functions and could run though a (expertise) leveled escalation procedure aligned to a corporate product or problem (diagnostic) domain. Practitioners working at the different levels of support shared solution knowledge even if separated by distance and time zones as long as trust existed between the practitioners (Davenport & Prusak, 1998). Therefore, as in literature, the theories that conceptualize culture do so in terms of reference group value orientations (Jackson, 1995) such as value dimensions at the organisational and functional levels (Jackson & Philip, 2010). These functional levels in CME-Co and TELE-Co have had an impact on the behaviours of firm members by creating a social control environment that sets the expectations and boundaries of appropriate behaviours for the different group practitioners (Wenger & Snyder, 2000). CME-Co boundaries are very much domain and trust specific as skilled support Engineers are denied access to Engineering knowledge reservoirs. However, an intern with little experience and technical knowledge is given access when assigned (access rights) to the Engineering domain (Dhillon, 2006).

Culture was an obvious enabler of KM in the two case organisations (Davenport & Prusak, 1998). A supporting organisational culture helps motivate practitioners to share knowledge and find the time for KM. Enabling employees to share knowledge was, as reported, the hardest aspect of KM (Becerra-Fernandez et al., 2004). The culture that is conducive to KM is likely to value elements such as networking internally and externally, respect for individuals, creativity and innovation, trust, sharing ideas and information, sound underlying systems and procedures, and continuous learning and development. However, even though, the two case organisations exhibited all of these aspects of a KM enabling culture, it was to varying degrees. The support functions were

very dependent on the internal and external networks with CME-Co pushing knowledge towards their customers to be more competitive and TELE-Co more aggressively targeted regulatory and academic forums then trusting external partners. Communities of practice were used, while unofficially in TELE-Co, between trusted parties to promote quality and sharing (Buchel & Raub, 2002). This difference could easily be attributed to the fact that CME-Co's CS function has been pushing and pushing the benefits of KM to support customer needs and reduce operational costs (Coakes, 2004; Brelade & Harman, 2003). As a result a gradual increase in access rights to Engineering solutions and bugs were provided and KM roles (knowledge consultant and knowledge writers) and communities of practice (knowledge development group) were created. Perhaps, with time, the TELE-Co PKM group will expand and become a formal CoP. Attributes of an enabling organisational culture include understanding the value of KM practices, management support for KM at all levels, incentives that reward knowledge sharing and creation (Hislop, 2005; Orlikowski, 2002). This attribute varied from one case organisation to the next. CS in CME-Co understood the value of KM practices (proved through cost reductions); support existed at high levels in the CS organisation (within CME-Co) but was very much controlled by the Engineering function. The incentives for all employees were identified after a trial and error process of determining the most effective. Monetary rewards were eliminated after the number of solutions created increased and quality was reduced. CME-Co allocates an expert or guru status to practitioners who share valuable (used solutions) knowledge. TELE-Co's KM initiative is very much on an ad hoc basis. The value of KM is understood but not officially supported within the CS and Engineering domains.

These same cultures enabled individual and function hoarding, limited employee interaction and lack of managerial support in CME-Co and TELE-Co which inhibit knowledge sharing. Davenport and Prusak (1998) identified a number of cultural factors that act as inhibitors or frictions as they can slow the process of sharing knowledge down. Table 7.1 outlines the different types of frictions that have been identified in the two case organisations and the approaches used to solve them. By being aware of these frictions organisations can avoid them. There is a complete lack of trust between the CS and Engineering domains and more so between Engineering and CS than with the other corporate functions within the two case organisations. CMC-Co has identified the problem and encourages face-to-face meetings and when possible job shadowing or rotation. TELE-Co utilises mentoring but is not as proactive as CME-Co in addressing the issue of trust and individual hoarding. It is one of the responsibilities of the knowledge consultant to drastically reduce hoarding in the CME-Co CS function.

FRICTIONS	SOLUTIONS
Lack of trust	Build relationships and trust through face to face meetings
Different cultures, vocabularies, frames of reference	Create common ground through education, discussion, publication, teaming, job rotation
Lack of time and meeting places; narrow idea of productive work	Establish times and places for knowledge transfers, fairs talk rooms, conference reports.
Status and rewards go to knowledge owners	Evaluate performance and provide incentives based on sharing
Lack of absorptive capacity in recipients	Educate employees for flexibility provide time for learning, hire for openness to ideas
Belief that knowledge is prerogative of particular groups, not invented here syndrome	Encourage non-hierarchical approach to knowledge; quality of ideas more important than status of source
Intolerance for mistakes or need for help	Accept and reward creative errors and collaboration; no loss of status from not knowing everything

Table 7.1: Knowledge Transfer Inhibitors (Source: Davenport & Prusak, 1998).

The two organisations have strived to foster the corporate culture through training, common terms of reference, practices and on-the-job mentoring. The issue of having time to transfer knowledge is targeted officially by CME-Co through regular demonstrations of the eventual time saved by sharing knowledge. In escalated levelled support if knowledge is pushed down to the lower levels time will be saved at the higher levels for more important processes such as innovation. Additionally, by reducing the numbers of levels a problem is raised to - the cheaper the operation. External knowledge transfer is supported in the two organisations through participation in conferences, symposiums and regulatory bodies. CME-Co evaluates performance and allocates status to practitioners who share, TELE-Co does utilise employee reviews but knowledge sharing is not evaluated (conducted by managers). The practitioners in the two case organisations have a high absorptive capacity and are hired for their ability to innovate. A non-hierarchical approach to knowledge is understood yet not encouraged across functions. The Engineering functions in TELE-Co and CME-Co have a high sense of importance in themselves. Unfortunately this is encouraged at senior levels within the two case organisations. CS and ISS in CME-Co have encouraged the fact that it is the quality of the ideas that are more important than status of the source. The use of learning from mistakes is encouraged in ISS through the auditing process. Post-mortems are carried out after a review to identify mistakes and learn from the different lessons gained in order to improve. This post-mortem analysis is very much aligned to the literature (Baskerville, 2008) as lessons can be learned from mistakes.

However, outside of Engineering and CS the other functions, including ISS, in the two case organisations, did not utilise KM. ISS have benefited from the enforced sharing, documented processes, best practices and evaluations which have resulted in similar benefits to the CS KM initiatives used but are a direct result of the impact of compliance. Compliance (and the implications of non-compliance) has endowed ISS with a separate structural, political (senior support) and budgetary identity in CME-Co and TELE-Co. Therefore IS Security culture is composed of more than the confidentiality, integrity and availability of messages (Dhillon, 2006). Policies and procedures which are clearly articulated and supported by management are a good mechanism for setting the cultural tone regarding risks (Greenstein & Feinman, 2000). Beliefs and best practices influence the behaviour of employees regarding IS Security (Thomson & Von Solms, 1998; Hu et al., 2008) and as a result staff should be aware of procedures aimed at preserving IS Security of corporate assets. It is vital that IS Security awareness is instilled in the culture of an organisation (Ettinger, 1993) by the IS Security function and management (Borodzicz, 2005; Dojkovski et al., 2007).

The cultural theory literature argues that a practitioner's position can be controlled by the functions in which they work (Jackson & Philip, 2010). As argued by Douglas (1970), who recognised that belonging to a group can place constraints on how people behave, CME-Co and TELE-Co exhibited cross functional conflict and knowledge hoarding. As explained by Jackson and Philip's (2010) cultural cosmologies (outlined in section 2.3.4) the two case organisations display elements of three of the four types. Hierarchism is characterised by strong grid and strong group. There was a strong emphasis on order, discipline and coordination of tasks in the ISS and CS functions of the two case organisations. This provided visionary leadership and coordination in achieving IS Security and CS targets. However, Engineering tended to have too much control and power and smothered CS and ISS (through the circumvention of controls) vision, fostered dissatisfaction, ultimately leading to an impassive cultural orientation (Tolsby, 1998). Individualism/Market was also evident as there were opportunities for creativity and innovation. In its constraining form it created a culture where individuals

seized opportunities to their own advantage, leading to non-collaborative behaviour (Tsohou et al., 2006) in the form of knowledge hoarding. However CME-Co has taken formal steps to avoid the constraining elements of individualism. Egalitarianism was strongly evident in the two case organisations. Functional concerns took priority over individual practitioner interests. Members stressed the importance of group-ethos, teamwork and trust. At a functional level it fostered knowledge sharing, teamwork and trust to exist between functional members (Adler, 1991). However neither of the two case organisations exhibited this at an organisational level. Functional conflict regarding knowledge sharing was constant. Change can only be effective if individuals are willing to work as part of a team/group. In its constraining form, egalitarianism due to its lack of leadership and authoritative values, can lead to breach of trust and unsettled disagreement and internal corporate rivalry which can if unchecked have negative implications. Neither of the two case organisations demonstrated fatalism which results in values of apathy and fear. This creates a hampering environment to transcend throughout the organisation in times of change (Kaarst-Brown & Robey, 1999) possessing no enabling characteristics.

Therefore ISS managers should strive to reduce constraining cultural characteristics and create a facilitative IS Security environment by promoting the enabling cultural values. As described by Jackson and Philip (2010) organisations require the drive and innovation of individualism/market for enhancement and improvisation; the visionary leadership, resources and coordination of hierarchism, and the teamwork, trust and knowledge sharing of egalitarianism. This view is supported by a number of researchers (Ruppel & Harrington, 2001; Hendriks, 1999; Adler, 1991). However, membership of a cosmology is not fixed or permanent. It is dynamic as an individual could be a member of multiple cosmologies at the same time and drift between them. This was very much evident in the communities of practice identified in the two case organisations (as discussed in section 7.1.4).

7.1.2 Interpreting the use of Common Knowledge in the Case Studies

The two case organisations utilised common terminology (knowledge) to integrate employees into the TELE-Co and CME-Co cultures. This approach enabled a common communication platform in order to foster competitive cultures. The case organisations utilised corporate universities (CME-Co and TELE-Co Universities) to, not only, develop their employees skill-sets but to teach the common corporate knowledge used in Engineering, CS, IT and IS Security. The two case organisations used M-Gates and Six Sigma to ensure all employees utilised the same terminology in collaborating and managing projects across the different business and support functions. Additionally, the two organisations offered a wide array of complex products to their customer bases. Product designs and specifications were considered common knowledge in the technological functions. The corporate Intranets were used to publish general or common knowledge pertaining to corporate procedures or newsletters, contact lists, presentations, policies and best practices were stored on functional websites. The case organisations also used enterprise-wide KM initiatives in the form of content management systems to act as central document repositories. The IS Security functions used SETA induction courses to introduce new hires to the different corporate security risks, policies and penalties for policy breaches. It was the intention of the different induction and training programmes to educate new hires in behaving like a TELE-Co or CME-Co employee.

7.1.2.1 IS Security Common Knowledge

In literature common or general knowledge refers to cumulative experiences which support communication and coordination through: language, vocabulary, recognition of individual knowledge domains and shared norms (Grant, 1996). This approach provided a sense of unity to the members of the two case organisations. The corporate universities helped enhance the value of individual expert's knowledge by integrating it with the knowledge-base of existing TELE-Co and CME-Co employees. These two engineering organisations used terminology regarding the development status of a product, modelling terms, M-Gate requirements when discussing project management and technical terminology regarding ISS technologies, vulnerability levels and the corporate rule base (for monitoring software and firewalls) and standards. Common CME-Co and TELE-Co knowledge was owned by the majority of the employees and was easily transferred through KM mechanisms. However it was specific to each organisation. The value of an expert's knowledge increases once integrated, as is cannot be shared with the organisations competitors, thus impeding knowledge leakage (Argote & Ingram, 2000; Becerra-Fernandez et al., 2004). Finally, common knowledge can aid in creating a competitive environment and overall corporate culture of the organisation (Bennet & Bennet, 2004).

Therefore common knowledge was used, as stated in literature, as an approach to creating a corporate culture driven towards competition across the two case organisations (Hislop et al., 2000; Buchanan & Gibb, 2008). However CME-Co purchased best practices (such as M-Gates) to utilise industry recommended terminology as opposed to enhancing the corporate common knowledge base and therefore enabling the transfer of core knowledge outside of the organisation instead of retaining its value within. While TELE-Co did create common knowledge and operating procedures it also shared these with its industry competitors and partners to create and expand industrial common knowledge in order to enhance industrial standards and therefore market and product interoperability.

7.1.3 Interpreting the Physical Environment in the Case Studies

The two case organisations are multinational organisations with subsidiaries located throughout the world. CS, IS Security and Engineering functions were also distributed throughout the different subsidiaries to support the needs of internal and external customers. CME-Co, in one subsidiary, used an open-plan layout to allow CS employees to collaborate in problem-solving. However when a problem was escalated to Engineering the customer call was diverted to the U.S. creating a physical barrier to sharing knowledge through distance and different time zones. Face-to-face problem-solving was regarded by TELE-Co and CME-Co CS and IS Security functions as an imperative to building collaborative relationships. To reduce the negative aspect of this physical environment the functions used job rotation and shadowing to send new hires to corporate head quarters in order to build relationships. Additionally, meeting rooms were used to brainstorm ideas or conduct post-mortems for quarterly and yearly audits. These distributed physical environments were also a security challenge. Securing a corporate network which has subsidiaries scattered around the world is an enormous IS Security undertaking. In order to protect geographically dispersed subsidiaries the IS Security functions utilised Security Officers or Coordinators. Such roles had the responsibility of rolling-out selected ISS standards and controls identified by the corporate ISS groups. They collaborated by using a number of KM mechanisms (Table 7.2) provided by TELE-Co and CME-Co. Physical security adds to the issue of the

physical environment. The two case organisations utilised a security presence in the form of guards and access (swipe) keys to remind employees and visitors of the different environmental risks. However, TELE-Co was far more stringent in enforcing penalties for physical security checks regarding employee responsibility. This was a physical reminder to employees that they should always be aware of security risks. However many employees reported that this and other controls were not regarded as barriers to sharing knowledge or as a security reminder as they eventually became transparent after a few weeks to new hires.

7.1.3.1 IS Security Physical Environment

The physical environment in TELE-Co and CME-Co was identified by the different practitioners as important as it allowed them to meet and share ideas and knowledge. It includes the physical layout of the buildings used by the two case organisations, how the different buildings and organisational functions were separated and the forums used to enable employees to collaborate. Web-based forums were used by the two case organisations to bypass the distance barrier, in order, to share knowledge through collaborative platforms such as E-Room, Compass and vendor repositories providing opportunities for practitioners to meet and share ideas (Becerra-Fernandez et al., 2004). In the literature it was reported that most employees acquired their knowledge from informal conversations with their colleagues as opposed to training or standard operating procedures (Wensley, 1998). CME-Co in particular identified the importance of job rotations and shadowing to transfer knowledge between the different levels of problem-solving support. However, neither case organisation intentionally created spaces for their employees to meet face-to-face and share knowledge as advised by Stewart (2000). Therefore the physical environment can foster or impede knowledge sharing. In contrast to the literature, regarding the importance of the physical environment for knowledge sharing, both organisations were constrained by distance and the different time zones. While job rotations and IS Security coordinators (positioned within each subsidiary) were utilised, neither could replace the advantage of face-to-face problem-solving.

7.1.4 Interpreting Structural Requirements in the Case Studies

The structure of the two case organisations is complex. The difficulty in managing dispersed geographies makes the reporting process complex. CME-Co is a multinational that has grown from small to a large organisation very quickly. This growth has resulted in an approach to the management of knowledge which mirrors that of a smaller organisation, with specific departments such as Engineering reluctant to share knowledge. TELE-Co too has rapidly expanded, “resulting in a convoluted mess”, and like CME-Co it is dominated by Engineering. Commercial drivers have forced CME-Co to divide its core customer functions into two. Customer Support sits in between Engineering and CME-Co customers. This structural model has resulted in a reluctance to share knowledge (product designs, coding errors) between Engineering and Customer Support due to the perceived risk of CS passing product designs and bugs onto customers. TELE-Co aligns CS regional teams to divisions which are categorised according to the different products developed by the company. Engineering and CS are reluctant to share knowledge with one another and with other organisational units such as Marketing due to the same perceived risk of code (or dangerous commands) becoming public knowledge.

CME-Co has analysed its organisational structure to reduce the number of managerial layers needed for decision-making and reporting in each geographical location. This change resulted in creation of one umbrella role for specific products ensuring the customer, through one knowledge channel, was provided with the following: one contact, the same content, (terminal) console and information pertaining to the problem raised. This avoids the scenario of a customer requiring access to multiple files and more than one Technician. This was common when support responsibility, due to multiple CS teams, was varied for interoperability problems. Additionally, CME-Co removed core functions such as the Help Desk support from its international subsidiaries to centralise the organisation even further in order to reduce costs and dependency on corporate subsidiaries. TELE-Co, at the time of undertaking this study, was in the process of re-evaluating its structure and reducing the number of in decision-making layers as, like CME-Co, it has created problems. TELE-Co was divided into five separate divisions across the globe under the WEC (World Engineering Corporation) umbrella and very much separated according to product development and support.

The two case organisations have established formal IS Security functions with political, structural, and budgetary independence from the corporate IT function. This change in the corporate structure and strategy of the cases was due to external, environmental drivers (in the form of regulatory changes) and customer demands. The cases were proactive in ensuring compliance with the required regulations to operate across different geographies but also in identifying customer demand for security enhanced products and services. CME-Co established the OISRM to source regulatory guidelines and best practices. These were then customised as CME-Co branded guidelines and best practices for internal use. The IS Security function within CME-Co was separate from the GIS function but reported to the Global IS Director in the U.S. who reported to the Chief Information Officer who in turn reported to the Chief Financial Officer. Locally security was managed by IS Security Officers who were responsible for the security needs and audit reviews of individual sites. IS Security was divided into two fundamental groups operating within corporate headquarters and dispersed throughout the multinational. The Corporate Security group represents CME-Co stakeholders and (customers, shareholders, and partners) by identifying their product, service needs and aligning security to the strategy of the organisation, driving the development of security enhanced tools and identifying customer compliancy needs. Customers (large multinationals) were unsure of their regulatory preparatory needs regarding technology and standards. The Corporate Security group identified this as a potential market and has aggressively targeted it. Therefore CME-Co has raised the profile of the IS Security function structurally, politically and strategically due to environmental requirements and potential monetary gain.

The new reporting structures in the two case organisations required ISS to report to the Finance and legal departments. External reviews from auditors and consultants has forced a significant change in the importance of the two IS Security functions. TGS like OISRM resolve security-related problems by improving IS Security processes which ensured a secure infrastructure for employees through proactive security strategies (policies, secure technologies and business assessment methodologies). TELE-Co also created a group (TIPs) responsible for developing global security procedures and policies which were disseminated to the various subsidiaries. Customer Support and Engineering are key strategic units within CME-Co and TELE-Co operating like silo organisations servicing customers throughout EMEA and APAC. The IS Security functions support their infrastructural and communication needs.

However due to the status of Engineering and CS, in the two case organisations, members of these units regularly circumvent security controls in order to access specific knowledge or experiment in their labs[23]. This creates weak points in the corporate network making backdoors available to potential hackers and affecting the stability of the corporate networks. Therefore despite the new structural and strategic status of the IS Security functions their position was irrelevant in a multinational with an Engineering dominated culture.

7.1.4.1 IS Security Structural Requirements

The management of IS Security depends, to a considerable extent, on the structures of CME-Co and TELE-Co. Traditional reporting relationships influenced the flow of data, information, knowledge, the nature of decision-making and in sharing knowledge across the different functions (Dhillon, 2006). Organisational structures can cause more complicated process flows compared to hierarchical structures. Knowledge sharing was facilitated when CME-Co was more decentralised (Borchgrave et al., 2001). TELE-Co's convoluted structures caused more complicated process flows compared to hierarchical structures (Borchgrave et al., 2001). A further layer of complexity was added when the two case organisations established relationships with other enterprises (Gal-or & Ghose, 2005; Dhillon, 2006). TELE-Co utilised collaborative relationships to steer the industry while CME-Co additionally utilised partner knowledge to expand the corporate knowledge-base and reduce CS operating costs. While the ISS functions in the two case organisations extensively utilised collaborative partnerships with vendors to adhere to regulations and source the best practices and standards as reported in the ISS literature (Stewart, 2005). ISS in TELE-Co and CME-Co allocated a number of ISS countermeasures in managing increasingly complex security architectures to support these collaborative partnerships (Gal-or & Ghose, 2005).

The organisational structures in CME-Co and TELE-Co facilitated knowledge sharing through formal and informal communities of practice (CoP) mirroring the structures identified in literature (Wenger & Snyder, 2000). These communities of practice provided access to external knowledge sources such as vendors and in CME-Co stakeholders (Belsis et al., 2005; Stewart, 2005). These external stakeholders were often a greater source of ISS knowledge than the organisation itself. One of TELE-Co's informal communities of practice, PKM was informally created by design Engineers to manage and promote KM. CME-Co created formalised CoP to properly coordinate and control their activities internally with the KDG (Knowledge Development Group) and the KCS (Knowledge-Centred Support) communities of practice. The corporate security group was established to form extended communities of proactive between the CME-Co and external stakeholders for the sole purpose of identifying security opportunities. This contradicts Kimble and Hildreth's (2004) question regarding whether communities of practice are always suitable for the business setting, arguing that their interests may not be aligned with those of the organisation. The CoP in CME-Co were formally created and were directly aligned to the needs of CME-Co. TELE-Co's KM CoP was informally created to take advantage of the benefits of KM. CME-Co and TELE-Co workers do, to a point, operate in an individualistic manner to obtain resources through personal networks and individual relationships but in order to solve function specific problems. This corroborates Pan and Leidner's (2003) goal of utilising KM initiatives to develop networks where knowledge is shared and used by developing communities of practice (CoP). New knowledge is constantly created through for example auditing and

[23] Engineering networks are separated using a DMZ. Two firewalls are used to partition sections of the corporate network.

collaborating with vendors (Davenport & Prusak, 1998; Wenger & Snyder, 2000). KM mechanisms such as: a knowledge champion (TELE-Co's PKM) or a knowledge consultant /champion (CME-Co's KDG and KCS) were facilitated through a variety of communications tools such as e-mail, telephone, or groupware.

Specialised structures and roles, such as the IS Security functions, specifically support organisational operations (Brown & Magill, 1994; Strassman, 1995). The individuals responsible for IS Security are vital in ensuring the success of any plan to prevent known threats and respond to unplanned incidents (Im & Baskerville, 2005). ISS methods, strategies and procedures ensured the protection of the resources of the two case organisations. Therefore the IS Security policies in TELE-Co and CME-Co functioned as guides These will then be the basis for formulating policies or strategies and procedures for risk and IS Security management (Baskerville & Siponen, 2002; Booz et al., 2005; Jones & Ashenden, 2005). The IS Security function structure attempts to match corporate objectives by supplying a complete framework for planning and developing in TELE-Co and CME-Co through OISRM and TGS. The assignment of authority and responsibility through ISS governance is an extension of the structures of the two case organisations (Kaen, 2003; Sundt, 2006).

The organisational structures in TELE-Co and CME-Co strongly influenced the implementation of IS Security activities and the consistency with which they facilitated the enterprise's goals. The role of senior management is to guarantee that its structure is supportive of the deployment of security-related initiatives, without necessarily impeding business processes. This was evident in CME-Co's collaborative relationships with partners and vendors as sensitive processes, through the extranets, were separated into different entities and more secure measures (such as VPNs) were established specifically for them. Finally, the two case organisations followed advice from industry and academia in separating the ISS function from IT and in the case of CME-Co a senior ISS role was created specifically to source and coordinate the implementation of ISS standards and practices (Dutta, & McCrohan, 2002).

7.1.5 Interpreting IT Infrastructure s used in the Case Studies

CME-Co uses a number of communication technologies to collaborate (section 7.2.4). Logical access rights are used to control the provision of access to CME-Co and TELE-Co knowledge stores. CME-Co provides its customers with an integrated infrastructure package to enable them to utilise their storage platforms more effectively, therefore to consolidate multiple data centres into possibly one (section 7.2.2.1). Security was used to enhance these product offerings in light of the regulatory requirements already described. TELE-Co does not target customers with corporate infrastructural solutions (unless the requirement was a wireless, mobile problem). The two case organisations availed of content management systems to store lessons-learned and documentation. Information systems were used extensively to support knowledge capture and reuse (section 7.2.3). Additionally, the two case organisations required a global security infrastructure with roles allocated to the different categories of security (section 7.3). Collaboration was enabled through call conferencing, video conferencing, the Intranet, email and the corporate Intranets.

7.1.5.1 IT Infrastructure

IT infrastructures of the two case organisations include data processing, storage, systems and information communication technologies (ICT). This framework connected

the practitioners of the two organisations to the different internal and external knowledge and processes (section 7.2). It was the IT and ISS infrastructures which secured the organisations and assured the value and utility of the different knowledge reservoirs (section 7.2.3; Figure 7.7(b)). The infrastructures secured and supported the processes, people and technology involved to prevent unmanaged organisational knowledge (Holsapple & Singh, 2004; Jamieson & Handzic, 2004; Belsis et al., 2005; Randeree, 2006) in CME-Co and TELE-Co. The type of infrastructure utilised determined the level of access ISS and CS practitioners had to the knowledge located in CME-Co and TELE-Co, the amount of knowledge that was communicated through platforms (section 7.2.4) the richness of the communication mediums such as Primus in CME-Co and Compass in TELE-Co and the aggregation of data from multiple sources through the internal and external platforms.

Technological changes, in both secure hardware and software, are as constant as the increase in the number of threats to corporate security (section 2.4). Secure protocols, standards and encryption were used to protect business environments (Stallings, 2001; Dhillon, 2006) and security technologies such as firewalls, scanning tools and intrusion detection systems were used to filter out possible threats (Jamieson, 1991). Virtual private networks were used by the case organisations to encrypt communication lines with external customers who were risk assessed and controlled through NDAs. CME-Co utilised a mesh of controls to create a secure tunnel between its partners and its internal resources. Theoretically the data derived from the tools used should, if utilised correctly, provide an integrated view of knowledge pertaining to the security landscape of the two organisations (Belsis et al., 2005). CME-Co and TELE-Co (in particular) pulled the data from its multiple monitoring tools and software into tracking databases to aggregate the data and build a picture of the security landscape (Stewart, 2005) to improve the security of the environment (Whitman & Mattord, 2005) when implemented.

7.1.6 Interpreting the Case Studies Business Environments

The two case organisations operate in a business environment influenced by rapid technological advancement, high demand and short product lifecycles and therefore a high level of uncertainty (Tables 5.1 & 6.1). Threats such as reverse-engineering, viruses and regulatory constraints were considered significant. CME-Co and TELE-Co were effectively being bombarded by regulations. As U.S. multinationals with overseas subsidiaries the two case organisations were required to comply with local, State and Federal laws in the U.S. and E.U. regulations in their international markets. CME-Co and TELE-Co operate in a fragmented security market sector with over three hundred security companies supplying hundreds of different security (compliance) products which have made it very difficult for companies, including CME-Co and TELE-Co, to select suitable technologies. This was compounded by the fact that the only compliance advisors (regarding security technologies) were vendors. As a result CME-Co identified the competitive opportunity of incorporating security add-ons to their storage product portfolios and in offering compliance related knowledge-based activities.

CME-Co regards competition as a means of learning, regularly comparing the company's performance with its competitors in order to drive its workforce. As a result KM was identified as a strategy that would allow the company to efficiently use its internal and partner knowledge. A CBR was used to pull knowledge from the external environment to act as a source of competitive knowledge. CME-Co identified compliance as an opportunity to full-fill customer's storage and regulatory needs. As a

direct result the CME-Co product portfolio became wider and more complex. Its stakeholder group (the Corporate Security Group) provides significant expertise in identifying and supporting customer needs. TELE-Co's engineering teams identified KM as an approach to manage knowledge across the different design domains. Through the use of an informal community of practice the function utilised KM to manage product development resources efficiently and to coordinate the different facets of Engineering. However the focus of the initiative was purely to drive collaboration between the different design domains as opposed to all of Engineering, the CS function, customers or any other part of the organisation. This did not enable knowledge sharing across the organisation. It was team specific as opposed to function, as is the case in CME-Co.

Evolving with their business environments was an imperative for the two case organisations. CME-Co targeted the market and identified niche areas to develop products which incorporated compliance needs into designs. Additionally CME-Co used its KMS to push knowledge (solutions) towards its partners and customers. Therefore the goal of the two case organisations was to keep pace with the rate of technological change in their respective business environments. This did provide significant challenges while operating in the telecommunications and storage industries. Deregulation has changed the business landscape of the two case organisations, resulting in competition from a wide range of telecom service providers (for TELE-Co) and technological companies diversifying into new markets such as storage (for CME-Co). Finding and retaining customers was (and is) vital. The main challenge was to understand and identify customer requirements and then to satisfy them. The ISS and CS Support functions were, as a result, crucial for the two case organisations in their interactions with their respective business environments.

7.1.6.1 Business Environments

The ISS activities of the two case organisations affected not only the organisations themselves, but also their inter-relationships (Von Solms, 1999). The more sensitive knowledge, when communicated to a partner, was transferred via encrypted tunnels (CSI/FBI, 2005; Sundt, 2006). Deficiencies in IS Security can cause direct negative consequences for business processes due to errors, delays and information leakage (Jamieson & Handzic, 2004; Booz et al., 2005; Dhillon, 2006; Jones & Ashenden, 2005). However, the ISS functions operating within the two case organisations were slow to report deficiencies (Kaarst-Brown & Kelly, 2005; CSI/FBI, 2006). CME-Co did highlight the weakness created through the allocation of controls to Engineering and neglecting other functions which inevitably created weak points in the corporate network, a warning identified by Dhillon (2006). Such Failures in IS Security can temporarily deny network resources to employees and hackers can then use one organisation's resources as a stepping-stone in attacking another organisation (Dutta & McCrohan, 2002).

To make effective decisions regarding IS Security, management must know about the various threats facing CME-Co and TELE-Co, their employees, data, information, knowledge and systems. Thus, knowledge of threats and attacks are crucial to management when allocating resources, formulating security policies and performing risk assessments (Jones & Ashenden, 2005). This was reported as a difficult task by the ISS functions. The changes made to comply with regulatory requirements did force the functions to acquire ISS knowledge externally from vendors, retrieve ISS from the ISS technologies, create filtered reports highlighting internal and external threats, share this

knowledge across the dispersed ISS functions and apply the knowledge for reviews and to ISS strategies. While reported in the ISS literature as a necessity it was not identified as an advantage in enforcing compliance processes (Kaen, 2003; Chou, 2005; Sundt, 2006). The organisations encountered numerous IS Security challenges, such as: a rapid expansion of the enterprise ecosystem through external partnerships and new global markets, a value migration from the physical to information-based and intangible assets, continuing pressure to reduce costs (Booz et al., 2005; Dhillon, 2006), and compliance regimes (Butler & McGovern, 2008). The two case organisations identified these same challenges. However, the two ISS functions were positively impacted by the requirements of compliance as it significantly improved the management of ISS knowledge, provided political and structural advantages and increased the corporate revenue of CMECo through the offerings of knowledge-based services regarding compliance. CME-Co also identified the opportunity of utilising its external partnerships to create additional knowledge and therefore reduce support operational costs, contradicting the issues reported in the literature (Borodzicz, 2005; Gal-or & Ghose, 2005; Booz et al., 2005; Dhillon, 2006).

Organisations must design and create a safe environment in which business processes, procedures, employees and units can function. This environment must maintain the confidentiality, availability and integrity of the organisation's information and knowledge (Doyle, 1997; Jamieson & Handzic, 2004).These goals are met through the effective application of IS Security knowledge which is undoubtedly a critical resource for organisations (Escamilla, 1998) and the two case organisations.

7.1.7 A Synthesised Perspective on Organisational Infrastructure

The aim of this section was to determine how the organisational infrastructure could support the management of IS Security. Table 7.2 provides a summarised comparison of the two case organisations. Levels of the organisational infrastructure necessary to support the management of IS Security knowledge was evident in CME-Co and TELE-Co. However it was primarily due to the structural component of the organisational infrastructure. The two IS Security functions were formal departments which provided the IS Security functions with political status, resources and budgets separate to IT (Dutta & McCrohan, 2002; Dhillon, 2006). Environmental drivers, specifically compliance, has both raised the status of the function and forced the documentation of processes and collection of knowledge regarding the security landscape of the organisations for external evaluations. However this fact was not reported in the ISS literature. Furthermore, the positive impacts (Tables 5.12 & 6.12) gained from adhering to regulatory requirements for ISS were as significant as those of the KM strategies utilised in the CS functions.

Common organisational language and a culture of sharing were promoted in the two case organisations. The Engineering units in CME-Co and TELE-Co were and are reluctant to share knowledge due to the perceived risk of (design) knowledge becoming public or used incorrectly (high risk commands initiated in a customer environment). This conflict is a significant issue yet it is ignored by senior management. Barriers to sharing knowledge appear to be more historic than environmental. The CME-Co CS function was constantly battling to prove to Engineering and management the value of sharing knowledge through cost savings and as a result did gain more and more access to Engineering systems and solutions. External collaboration with CME-Co partners was proving effective in cutting costs in allowing customers and partners to "self-service" through the corporate Extranet. However TELE-Co and CME-Co used a

domain specific (role-based) approach to KM. That is, once a practitioner regardless of his/her expertise is assigned to a domain, access was provided to the functions knowledge reservoirs and blocked from experts working in other domains. Communities of practice were created for collaboration across the two case organisations in order to collaborate across units or through inter-relationships. CME-Co formalised its CoP to coordinate and control their activities to ensure quality standards and enhance practitioner skill-sets. TELE-Co utilised informal CoP to share domain specific knowledge. Therefore knowledge was pushed around the Engineering design domains and not to CS or the corporate customer base.

In the literature the importance of organisational infrastructure in supporting KM is high. Nevertheless, by overlooking the need to formulate a clear business case, many KM implementations fail (Coakes, 2004). Neither of the two case organisations support KM at a senior level beyond the creation of a corporate central repository. The co-ordination of KM requires the leadership of senior management if the organisation is to benefit from its utilisation. Even though many researchers highlight the importance of an overall KM strategy (Hansen et al., 1999; Choi & Lee, 2002; Malhotra, 2000; Coakes, 2004), it was not implemented in CME-Co and TELE-Co. KM has impacted CME-Co and TELE-Co directly and indirectly but only at functional levels. The literature has warned against companies isolating KM in functional departments such as CS (Hansen et al., 1999). The majority of organisations focus on the operational side of KM as opposed to an integrated approach. However the ISS functions did effectively (albeit indirectly) manage, due to the impact of compliance, their knowledge and benefited from structural, political and budgetary independence.

	ORGANISATIONAL INFRASTRUCTURE	
	CME-Co ORG. INFRASTRUCTURE	**TELE-Co ORG. INFRASTRUCTURE**
(1) Culture	• Promote a culture of Knowledge sharing • CoP battle to prove to management| Engineering the benefits of knowledge sharing • KM is an IT Solution at corporate level • Mentoring| Job Shadowing, Rotation| University • KM is function specific • Compliance has created an awareness of ISS • Compliance has raised the profile of ISS • Geographical spread| Time Zones| Language are barriers • Silo mentality regarding KM • Domain rights supersede trust	• Promote a culture of Knowledge sharing • CoP battle to prove to management| Engineering the benefits of knowledge sharing • KM is an IT Solution at corporate level Mentoring| Job Shadowing, Rotation| University • KM is CoP specific • Compliance has created an awareness of ISS • Compliance has raised the profile of ISS • Geographical spread| Time Zones| Language are barriers • Silo mentality regarding KM • Engineering snobbery supersede trust
(2) Structure	• ISS is structurally aligned • Complex structures with geographically dispersed subsidiaries • ISS function created to source external knowledge • Access rights are domain specific • No of managerial levels have been reduced to provide a better service to customers • Politically Engineering is a controlling unit capable of circumventing ISS controls and CS access rights	• ISS is structurally aligned • Complex structures with geographically dispersed subsidiaries • ISS function created to source external knowledge • Access rights are domain specific • Politically Engineering is a controlling unit capable of circumventing ISS controls and CS access rights
(3) Common Knowledge	• Used to build a culture of competitiveness • A corporate university is used to re-educate new hires into becoming CME-Co employees • Product portfolio • Engineering terms and methodologies • Stories of corporate legends	• Used to build a culture of competitiveness • A corporate university is used to re-educate new hires into becoming TELE-Co employees • Product portfolio • Engineering terms and methodologies
(4) Physical Environment	• Distributed subsidiaries Creates divisions through distance and time • Open plan offices • Face-to-face problem-solving is regarded as the best approach • Uses Job rotation to build relationships • Meeting rooms| teleconferences for brainstorming	• Distributed subsidiaries Creates divisions through distance and time • Open plan offices • Face-to-face problem-solving is regarded as the best approach
(5) IT Infrastructur	• ICT used predominately in supporting KM • KMS used to create, share and apply knowledge • Access rights are administered in a trail & error approach	• ICT used predominately in supporting KM • A central repository is used to share knowledge • Simulation SW is used to collaborate • Access rights are used to control knowledge
(6.) Business Environment	• Stakeholders drive the market • Membership of regulatory groups • CME-Co utilises a group to identify their needs • Dual role as a stakeholder driving the ISS market	• Stakeholders drive the market • Membership of regulatory groups •
	• Compliance has become a business driver • Membership of Regulatory bodies to drive market • Rapid technological changes • Pushes knowledge towards the customer • Learn from their environment • Targets the Fragmented ISS market • Threat of reverse-engineering	• Compliance has become a business driver • Membership of Regulatory bodies to drive market • Rapid technological changes • Pushes knowledge around an internal domain • Threat of reverse-engineering

Table 7.2: Organisational Infrastructure Characteristics.

7.2 Managing IS Security Knowledge

Sections 7.2.1, 7.2.2 and 7.2.3 describe: the different types of IS Security knowledge, reservoirs and processes identified in and across the CME-Co and TELE-Co case organisations. Section 7.2.4 describes and outlines (Table 7.2) the different KM mechanisms identified and section 7.2.5 compares the impacts gained across the two case organisations. The first part of each section interprets these variables across the two organisations. The second compares each to literature. Finally, section 7.2.6 concludes with a synthesised perspective of managing IS Security knowledge.

7.2.1 Interpreting the Types of IS Security Knowledge used in the Case Studies

This section describes the types of knowledge used within CME-Co and TELE-Co. IS Security (Sec) and Customer Support (CS) knowledge (K) are categorised as: general, technical and contextually specific knowledge. The roles of each type are identified as operational (O), tactical (T) and strategic (S).

General knowledge is used in day-to-day operations. CME-Co's IS Security and CS functions regarded hardware (HW) and software (SW) specifications, threats, email warnings, procedures and escalation levels as general operational knowledge. TELE-Co functions categorised organisational charts (roles and responsibilities), templates, and contact lists as such. Expertise in regulations, security technologies, systems, networking, procedures, checklists, policies, email notifications, assessment criteria's and threats were also identified as operational by TELE-Co. However the priority of hot issues and the approaches used to solve a problem were categorised as tactical by CME-Co's CS function (CME-Co Sec K= 0: CS K= 2). Hot issues are tactical as they can, if prioritised, provide tangible benefits such as: reduced workloads. Project management methodologies and prototyping-KM techniques, developed internally, were categorised as operational. Conversely, expertise in applying the techniques was categorised as tactical by TELE-Co (TELE-Co Sec K= 0: CS K=5). Reviewing the problem-solving process to increase productivity saves time as practitioners can prioritise and reuse solutions. The importance of expertise in applying step-by-step approaches to problem-solving is evident due to the necessity to combine and coordinate the creation of knowledge by practitioners.

Technical knowledge is specific to a function. Lists of errors and documentation are regarded as technically operational by CME-Co functions (CME-Co Sec K=4: CS K= 10). Regulations, product specifications, lists of stored solutions and errors, and knowledge of environments are fundamental. TELE-Co views its technical knowledge in designing new products, alerts, procedures and evaluation reports as operational. Knowledge pertaining to domains (access rights and designs), for the functions, while requiring expertise, is categorised as operational (TELE-Co Sec K= 7: CS K=13). Tactical IS security knowledge is used to implement regulatory constraints and in identifying risks to CME-Co systems. TELE-Co's IS Security function regards external forums, security controls, scanning and audit reports as tactical. CS views the ability to use knowledge from multiple sources as tactical knowledge (TELE-Co Sec K= 5: CS K=2). CME-Co regulatory knowledge was viewed as tactical as compliance is an environmental issue for the organisation. The CS function views its ability to diagnose interoperability problems and errors as tactical. However it is interesting that problem-solving is not viewed as tactical in either of TELE-Co's functions. IS Security in CME-Co has identified policies, regulations and strategies as strategic (CME-Co Sec K=5: CS

K=0). Security policies, strategies, and regulations and expertise in evaluating security technologies were regarded as strategic in TELE-Co (TELE-Co Sec K= 3: CS K=0). This can be attributed to the alignment of IS Security to the TELE-Co corporate strategy and the implications of non-compliance to environmental regulations. The security policy must be aligned to the strategy of the organisation so that it can manage known threats to the organisations. Regulatory knowledge is an imperative to CEM-Co as it has a dual role of protecting the organisation from internal risks and the risks associated with non-compliance. CS goals are not explicitly aligned to TELE-Co's or CME-Co's corporate strategies.

Contextually specific knowledge is viewed as tactical by CME-Co with audit reports and IS Security procedures as the organisations foremost resource. CS categorised its solutions and ability to solve problems as tactical (CME-Co Sec K=9: CS K=3) but primarily this knowledge is viewed by CS as operational (CME-Co Sec K=5: CS K=11). Contextually specific knowledge such as audit reports, lessons-learned, the reactive ability of IS Security experts and procedures were categorised as tactical by TELE-Co. CME-Co regards templates, product errors, solutions, bugs, lessons-learned and the steps to diagnosing problems as operational (TELE-Co Sec K= 9: CS K=5). However the ability to reverse-engineer is regarded as a tactical ability by CME-Co. Contextually specific knowledge was viewed as operational by TELE-Co (TELE-Co Sec K= 5: CS K=6). The differences in the TELE-Co ratios can be attributed to financial implications of not having the necessary expertise in applying regulatory controls, lessons-learned from audits and the inability to recognise risks (TELE-Co Sec K= 0: CS K=3). Thus, innovation is practitioner dependent.

The next section describes the IS Security knowledge identified and then compared to the literature.

7.2.1.1 IS Security Knowledge

There is a general consensus among theorists (Polanyi, 1966; Nonaka, 1994; Dieng et al., 1998; Coakes, 2004) that knowledge can be split into two different facets: (1) explicit and (2) tacit. Coakes (2004) posits that tacit knowledge is more difficult than explicit to codify as it is retained in people's minds and is not easily shared. Saint-Onge (1996) argues that the largest amount of knowledge within an organisation is tacit and is unarticulated. However, to be competitive CME-Co and TELE-Co must generate or create new knowledge. Explicit knowledge is viewed as knowledge that is codified, documented, archived and communicated. Explicit knowledge can be easily transferred from one place to another in a systematic and structured format (Alavi & Leidner, 2001; Coakes, 2004). The second classification of knowledge is between declarative and procedural knowledge. Essentially declarative knowledge is described as "knowing that" and procedural knowledge as "knowing what". The third classification of knowledge focuses on whether the knowledge is possessed widely or narrowly (Becerra-Fernandez, et al., 2004). Knowledge is also divided into support knowledge, which relates to the organisational infrastructure and facilitates the day-to-day operations; tactical knowledge, which relates to the short-term positioning relative to its business environment, competitors and suppliers; and finally strategic knowledge, which pertains to the long-term positions of the enterprise regarding its corporate vision and strategies in achieving the identified business goal (Patterson, 2005).

CME-Co regarded HW and SW specifications, threats, email warnings, procedures and escalation levels as explicit knowledge and necessary for everyday operations. TELE-

Co identified practitioner roles and responsibilities, templates, and contact lists as such. Each type easily codified and therefore transferred and stored. Tacit regulatory, technological and procedural knowledge was very much owned by practitioners. Therefore expertise in enforcing policies and regulations, identifying threats and the ability to proactively target alert notifications were regarded as tacit but operational to both case organisations. However the priority of hot issues and the approaches used to solve a problem were categorised as tactical by CME-Co. Hot issues are tactical as they can, if prioritised, provide tangible benefits such as: reduced workloads. Reviewing the problem-solving process to increase productivity saves time as practitioners can prioritise and reuse solutions. The ability in knowing how to apply the list and problem-solve the issues identified is a value-adding service. The importance of expertise in applying step-by-step approaches to problem-solving is evident due to the necessity to combine and coordinate the creation of tacit knowledge by practitioners. The documentation of the solution, by the practitioners in the two cases, allows this knowledge to be reused by other practitioners. This process contradicts the view of ISS knowledge in the literature (Belsis et al., 2005; Stewart, 2005, Randeree, 2006) as purely sourced from vendors.

Specific knowledge (technical or contextual) is possessed by a limited number of people and is both difficult and expensive to transfer (Hayek, 1945; Jensen & Meckling, 1996). Technically specific is deep knowledge about a specific field through both training and applied experience, and contextual refers to the knowledge of particular circumstances, such as an IS Security audit, of time and place in which tasks must be performed (Hayek, 1945) as it cannot be acquired through training. Knowledge can also be classified according to its role within organisations (Becerra-Fernandez, et al., 2004). Lists of errors and documentation are regarded as technically operational by CME-Co (CME-Co Sec K=4: CS K= 10). Regulations, product specifications, lists of stored solutions and errors, and knowledge of environments are fundamental. TELE-Co views its technical knowledge in designing new products, alerts, procedures and evaluation reports as operational. Knowledge pertaining to domains (access rights and designs), for the functions, while requiring expertise, is categorised as operational. Tactical IS security knowledge is used to implement regulatory constraints and in identifying risks to CME-Co systems. TELE-Co regards external forums, security controls, scanning and audit reports as tactical. CME-Co regulatory knowledge was viewed as tactical as compliance is an environmental issue for the organisation. However problem-solving is not viewed as tactical in TELE-Co. CME-Co and TELE-Co identified policies, regulations and strategies as strategic, which contradicts Wrapp's (1991) of the importance of each for strategic decision-making. This was due to the alignment of IS Security to the corporate strategy and the implications of non-compliance to environmental regulations for both case organisations. Contextually specific knowledge is viewed as tactical by CME-Co with audit reports and IS Security procedures as the organisations foremost resource with audit reports, lessons-learned, the reactive ability of IS Security experts and procedures were categorised as tactical by TELE-Co. This has been attributed to the financial implications of not having the necessary expertise in applying regulatory controls, lessons-learned from audits and the inability to recognise risks. Thus, innovation in the two case organisations is practitioner dependent as reported in the KM literature (Blacker, 1995; Gherardi, 2000; Orlikowski, 2002; Hislop, 2005) and not in the ISS literature (Randeree, 2006; Hu et al., 2008).

Figure 7.2 presents a synthesised representation of the different types of IS Security knowledge an organisation should utilise. The IS Security knowledge roles were not identified as this is very much dependent on the environment an organisation is

operating in (section 7.1.6). The arrows represent the eventual categorisation of IS Security knowledge as it is reused. Therefore, eventually contextually and technically specific knowledge will become IS Security general knowledge. The totals outlined in Tables 5.10 and 6.10 indicate that functional knowledge is viewed primarily as operational in the two organisations (CME-Co Sec K=20: CS K= 33 and TELE-Co Sec K=27: CS K=28). However, CME-Co IS Security knowledge was considered tactical (CME-Co Sec K=15: CS K=9). IS Security knowledge was viewed as slightly more tactical than CS knowledge (TELE-Co Sec K=14: CS K=12) in TELE-Co. The two organisations regard customer problem-solving as vital and knowledge intensive yet a fundamental operation (CME-Co CS K= 33 O| 9 T| 0 S). Neither organisation promoted or supported their Customer Support functions at a senior level. KM is utilised by the two CS functions but as ad hoc initiatives (TELE-Co CS K= 28 O|12 T|3 S). TELE-Co categorises the allocations of controls and problem-solving as operational knowledge, the application of regulatory requirements as tactical and IS Security policies and strategies as strategic (TELE-Co Sec K= 27 O|14 T|3 S). IS Security knowledge is regarded as strategic particularly vis-à-vis the security policies and strategies used by the two organisations (CME-Co Sec K= 20 O| 15 T| 5 S) (Dutta & McCrohan, 2002).

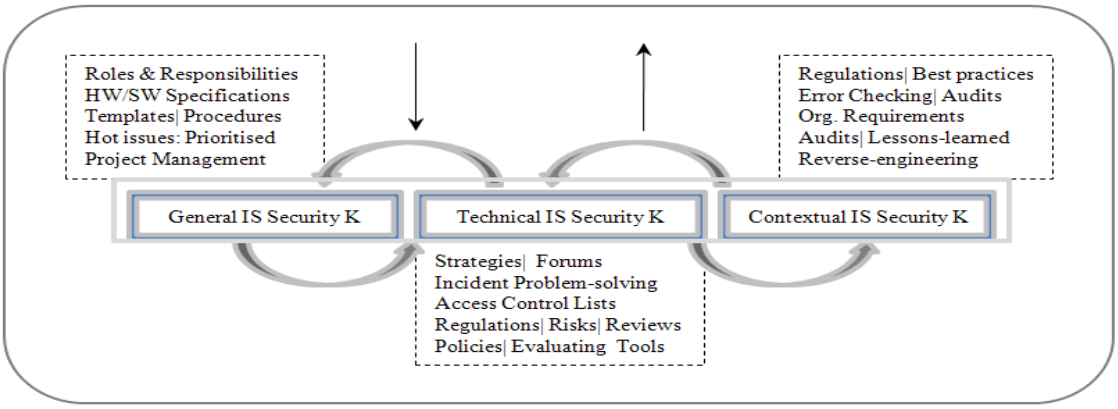

Figure 7.2: IS Security Types of Knowledge

The importance of IS Security knowledge can be attributed to the structures of the two organisations and their competitive business environments (Borchgrave et al., 2001; Dutta & McCrohan, 2002; Dhillon, 2006). IS Security is a futile function if it is absent from the organisational structure. The ability to identify and react to rogues (hackers) is also viewed as strategic, emphasising TELE-Co's recognition of its expertise in rectifying security incidents (Baskerville, 2004). However proactive strategies were not identified by either organisation as an important skill indicating an inability to be proactive in tackling security challenges (Dhillon, 2006). CME-Co has identified compliance as a niche market and as a result formed a group to target customer regulatory requirements and generate additional income. The steps in applying standards for regulatory requirements are vital to the function. IS Security practitioners utilised regulatory and control knowledge to ensure compliance and follow external advice regarding audits. The importance of IS Security is represented in the reporting structures which emphases the financial implications of IS Security and therefore its strategic importance in mapping IS Security to every business function, and process (Patterson, 2005). As a result knowledge use and development is therefore regarded as a fundamental aspect of activity (Hislop, 2005), making knowledge inseparable from human activity (Orlikowski, 2002). Equally, all knowledge work, whether using ISS knowledge, sharing ISS knowledge, developing ISS knowledge or creating ISS knowledge will involve an element of activity to ensure the value of ISS knowledge.

7.2.2 Interpreting the IS Security Knowledge Reservoirs used in the Case Studies

Knowledge pertaining to the functions of the two organisations is located in several different reservoirs. They encompass practitioners, artefacts and organisational entities. The reservoirs of knowledge are described and compared in the following sub-sections.

(1) The different roles and responsibilities attributed to **individual practitioners** of the two organisations were identified as significant sources of knowledge (Appendix D & Appendix F: Rows 1). Problem-solving specialists diagnose reverse-engineer and solve problems. CME-Co utilised specialists to identify stakeholder (customers and partners) requirements and as a result targeted the market demand for (product) security enhancements and regulatory solutions. A senior position was created (Director of GIS) in CME-Co to source IS Security standards and best practices and to formulate corporate guidelines for the organisation providing the IS Security functions with political power. The TELE-Co TGS umbrella function, through a coordinator, was reported to identify the IS Security requirements of the multinational. Security Officers are also used in two organisations as experts in each aspect of security from communications network to information. Internal and external auditors were used to evaluate and review corporate security by the two organisations. However TELE-Co used Export Managers to enforce and comply with U.S and international laws, specifically regarding encryption. The two organisations assigned experts to different levels of support. Expertise in product development, interoperability knowledge and diagnostic skills are regarded as valuable assets.

The cost of escalation problems has been analysed by the CS functions operating within the two organisations. To reduce costs knowledge management was identified as an approach to alleviate the pressure in fire-fighting and integrating product designs. CME-Co's CS function created an ad hoc Knowledge Consultant role to tackle the challenge of centralising CS knowledge. KDG Officers were appointed to identify the training needs of the different support levels. However, the roles are function-based. KCS writers were also allocated the responsibility of reviewing the quality of CS solutions. TELE-Co used a PKM Coordinator, on an ad hoc basis, to promote the application of KM in prototyping new products and designs. Therefore neither organisation formally recognises the role of KM and that it is function specific. However, IS Security is structurally aligned to the corporate strategy in the two organisations with CME-Co specialising in the application of IS Security knowledge in targeting niche markets (Stewart, 2005).

(2) The **function** reservoir of knowledge is an extension of the practitioner reservoir (Appendix D & Appendix F: Rows 2). Managers in the two organisations are responsible for identifying policies, standards and procedures. Security Officers and CS Engineers are used to coordinate the different subsidiaries in order to support operations. CME-Co and TELE-Co use customer feedback as a guide or measure for productivity and as a source of market demand. However CME-Co established a group specifically to target IS Security stakeholders. The two organisations have adopted specific approaches in securing corporate assets. Specialised groups were established as separate yet interacting entities to target key IS Security requirements. Groups (CME-Co's OISRM and TELE-Co's TGS) acquire and customise regulatory knowledge for dissemination throughout the multinationals and provide pools of expertise in compliance and IS Security controls. Security Officers, as groups, coordinate the roll-out of controls across the subsidiaries and collaborate on activities such as audits particularly in preparing for them and conducting post-mortems after the process has

ended. However CME-Co utilised a Remote Services group to assess and provide secure communication links to external partners. The two organisations utilise an escalation process to effectively exploit the tacit knowledge within CS and Engineering. Communities of practice were identified in CME-Co and TELE-Co within the CS functions. CME-Co has established a skill-set development and (solution) quality assurance groups to promote the management of knowledge within CS. A prototyping and knowledge management community of practice was created by TELE-Co Design Engineers to integrate knowledge across the different design domains. Thus, the two organisations CS functions established KM communities of practice which are function specific. However, while CME-Co has pushed knowledge towards customers and partners, TELE-Co's utilisation is internally focussed.

(3) Knowledge is stored in practices, routines and **procedures** within the two organisations (Appendix D & Appendix F: Rows 3). The IS Security functions utilised a number of procedures, standards, checklists and best practices to ensure CME-Co and TELE-Co's compliance to different environmental regulations. TELE-Co enforced strict use of its DMS to control the quality of the solutions created. ISO17799 was identified by the two organisations as a vital IS Security guideline. While the two organisations purchased and customised externally produced standards, TELE-Co created in-house policies as behavioural controls in terms of protecting the organisations proprietary information (POPI). Audit reviews were regarded as valuable sources of knowledge by the two organisations as externally sought evaluations of their IS Security functions. Review reports have been used as lessons-learned and checklists for the ongoing audit processes. M-Gates and Six Sigma were used by the two organisations as a common project management guideline and (gate) vocabulary reference model to ensure organisational consistency across projects. Usage varied within and across the organisations as CME-Co's IS Security function and TELE-Co's CS functions reported their use. However while the two organisations used the methodologies, CME-Co acquired them and TELE-Co created the tools.

CS templates were used to structure the standard operating procedures (SOP) enable effective searches and consistency. Bypassing steps in trouble-shooting can cost additional time if a call is escalated to another level of support. Prototyping as a methodology was used throughout CS and Engineering to test new designs and to learn from failures as well as successes. A limited number of procedures were used due to the closed environment in which the CS functions operate. However IS Security was described as cross-organisational support functions ensuring organisational adherence to policies and regulations.

CME-Co and TELE-Co used internal and external knowledge **repositories** (Appendix D & Appendix F: Rows 4). These were categorised as either paper-based or computer-based. The IS Security and CS functions, primarily, used the same repositories. DMS stored IS Security and CS solutions or fixes, which were accessed through the Intranet. The two organisations used vendor repositories to source manuals regarding security technologies, guidelines for incident recovery or product specifications in solving inter-operability problems (Belsis et al., 2005). The corporate IS Security functions exploited IS Security repositories to automatically pull (multiple) firewall, scanning and IDS logs located throughout the corporate network in order to collate filtered knowledge into a prioritised list of issues for Security Officers and coordinators. The CS function used managerial discussion forums in order to collaborate in formulating common procedures and goals. Notifications disseminated from Engineering, regarding "hot issues", or priority errors and solutions, were considered valuable sources of

knowledge. However access to CME-Co Engineering repositories was reported to be highly restrictive and resulted in partitioned knowledge. This is a necessary ISS countermeasure but it contradicts the advice provided by KM literature (Jamieson & Handzic, 2004). Engineering interviewees regarded the partitioning of the repositories as a fundamental approach to controlling their knowledge (product designs) and ensuring that any (known) risks which could seriously damage CME-Co's reputation were monitored (dangerous commands used incorrectly in a customer's environment). TELE-Co utilised external knowledge pulled from government repositories to comply with regulations in product development. CS also used public online forums to share coding solutions as an initiative to attract new hires. Therefore the IS Security functions used security repositories to automatically generate knowledge and CS used repositories to build and store solutions. However, the two organisations used E-learning tools to develop IS Security and CS practitioner skill-sets. E-learning resources were provided, through the two corporate universities, for online training courses. CME-Co in contrast to TELE-Co used portals to collaborate with partners and customers (E-Room and Power-link). Desktops and shared drives were also identified by CME-Co's IS Security function as individual function specific repositories. Subscriptions to technical repositories were used as a source of patch updates, procedures, and Q&A repositories.

(4) Knowledge was stored and retrieved in firm-specific **technologies** for day-to-day operations and other activities such as auditing (Appendix D & Appendix F: Rows 5). Email was reportedly used as a collaborative platform in problem-solving, accessing internal and external documentation and for storage throughout CME-Co and TELE-Co. The reported disadvantage to the utilisation of email was the difficulty in managing and retrieving solutions and documentation after a period of time. The IS Security functions exploited a number of security technologies to aid in monitoring and protecting their corporate boundaries. VPNs were used to encrypt lines of communication, SID for access-control and reporting, monitoring tools to generate alert logs, firewalls for enforcing internal/external access rules and IDS to track internal and external network traffic. Additionally, TELE-Co utilised Excel to create checklists and to calculate risk levels. Scanning technologies, such as ART and Found-stone, were used to monitor the TELE-Co corporate network and track employees and rouges. While, scanners were used in CME-Co they were not reported to be as highly valued as in TELE-Co. However, each IS Security technology generated streams of data which was pulled into monitoring databases in order to filter, query and generate a view of CME-Co's and TELE-Co's security landscapes. The CS functions utilised different technologies. CME-Co was very dependent on Primus, which was available across the organisation but only utilised by CS and Engineering. TELE-Co exploited simulation software and CAD tools to create models of new product and aid in decision-making. TELE-Co used a content management system (Compass) to centralise its knowledge across the different functions. Simulation tools were not used by either IS Security function to create and test decision-making in simulated scenarios.

(5) The two organisations displayed varying degrees of cross-**functional** interaction (Appendix D & Appendix F: Rows 6). CME-Co utilised a project management group as a collaborative mechanism across the functions. TELE-Co employed procedures (SRD) to stipulate the functional requirements of projects and the involvement of a Security Advisor to determine the level of risk to the organisation. The two organisations assigned the IS Security functions the task of determining the different roles and responsibilities of each employee. This task was necessary to enforce segregation of duties across the two organisations under the governance of the Finance and Legal departments. However, the CS functions of the two organisations interacted with a

limited number of units. CME-Co's CS function interacted with Engineering, R&D teams, ISS, IT and Sales. TELE-Co collaborated with Marketing as a source of technical expertise and as a control in protecting TELE-Co IP rights during sales pitches. The two case organisations regarded the CS functions as silos or corporations operating within the firm. Finally, the IS Security functions (transparently) supported every corporate unit and applied the controls necessary to enable and restrict employee access to systems, repositories, forums and KM. CS interoperates, as a technical advisor, with customer facing units to protect product designs and customer feedback.

(6) Collaborative partnerships or **inter-organisational relationships** were exploited by the two organisations as sources of IS Security and CS knowledge (Appendix D & Appendix F: Rows 7). Vendors were used to provide guidelines, product and technological specifications. The inter-relationships were formed to exploit financial opportunities. CME-Co established and utilised a Corporate Security group to analyse the security industry and identify stakeholder requirements. It was determined that the organisation could generate income through the incorporation of security tools and services into the CME-Co product portfolio and support. TELE-Co has hosted IS Security and CS symposiums to identify the direction of regulatory and market requirements. The two organisations have been active participants in regulatory bodies and IS Security forums to guide the market and create business opportunities. The forums consisted of networks of IS Security practitioners collaborating and exchanging details regarding attacks, best practices and standards. However, CME-Co enhanced their inter-organisational relationships through the use of collaborative forums such as Power-Link and E-Room. Knowledge was shared with customers as well as partners in order to generate solutions and reduce CS costs. The IS Security functions utilised external auditors as evaluators to adhere to regulatory requirements. The reports created were used as a form of measurement, a plan or checklist for future reviews and as a tool in post-mortem brainstorming sessions. The CS functions used customer feedback as informal review mechanisms. Knowledge collected from customers was used to alter product designs, remove flaws identified and the incorporation of potential trade-offs in product design. The two organisations exploited inter-organisational relationships to acquire market and regulatory knowledge and to ultimately manipulate the environments the organisations operate in.

The next section describes the IS Security knowledge reservoirs identified and then compared to the literature.

7.2.2.1 IS Security Knowledge Reservoirs

Problem-solving specialists diagnosed, reverse-engineered and solved problems. IS Security Knowledge reservoirs encompass people (individuals and groups), artefacts (practices, technologies and repositories) and organisational entities (organisations, functions, inter-organisational networks) (Becerra-Fernandez, et al., 2004). Drucker (1993) contends that knowledge is always embodied in a practitioner, created, augmented or improved, applied, taught and shared by a person (Argote & Ingram, 2000).

CME-Co utilised specialists to identify stakeholder requirements and as a result targeted the market demand for security enhancements and regulatory solutions. A fact not reported by the ISS literature as a value adding implication of compliance (Sundt, 2006) A senior position was created in CME-Co to source standards and best practices and to formulate corporate guidelines for the organisation providing the IS Security functions

with political power. TELE-Co utilised an IS Security coordinator to identify the IS Security requirements for the multinational. Auditors were used as experts to evaluate and review corporate security. The two organisations assigned experts to different levels of support. Expertise in product development, interoperability knowledge and diagnostic skills are regarded as valuable assets. CME-Co's CS function created an ad hoc Knowledge Consultant role to tackle the challenge of centralising knowledge. TELE-Co used a PKM Coordinator, on an ad hoc basis, to promote the application of KM in prototyping new products and designs. Therefore neither organisation formally recognised the role of KM and that it is function specific. However, CME-Co appointed a senior manager to align IS Security to the corporate strategy (Dutta & McCrohan, 2002; Dhillon, 2006).

A significant amount of organisational memory is stored in **organisational artefacts**. The IS Security functions utilised a number of procedures, standards, checklists and best practices to ensure CME-Co and TELE-Co's compliance to different environmental regulations. Audit reviews were regarded as valuable sources of knowledge by the two organisations as externally sought evaluations of their IS Security functions. Some knowledge is stored in practices, organisational rules, routines and procedures which are developed through experience over time, such as disaster recovery procedures (Levitt & March, 1988).

Knowledge stored in repositories and technologies represents other methods of storing knowledge in artefacts. Knowledge repositories can be paper-based, embodied in books, white papers, and procedures or web-based (Becerra-Fernandez et al., 2004). CME-Co and TELE-Co used internal and external knowledge **repositories** such as a documentation management system to store solutions. The two organisations used vendor repositories to source specifications in solving inter-operability problems. The corporate IS Security functions exploited IS Security repositories to automatically pull (multiple) firewall, scanning and IDS logs located throughout the corporate network in order to collate filtered knowledge into a prioritised list of issues for Security Officers and coordinators (Stewart, 2005). However access to CME-Co Engineering repositories was reported to be highly restrictive and resulted in partitioned knowledge. Engineering interviewees regarded the partitioning of the repositories as a fundamental approach to controlling their knowledge (Jamieson & Handzic, 2004) and ensuring that any risks which could seriously damage CME-Co's reputation were monitored. The two organisations used E-learning tools to develop IS Security and CS practitioner skill-sets (Gordon & DiTomaso, 1992; Dojkovski et al., 2007). CME-Co in contrast to TELE-Co used portals to collaborate with partners and customers (E-Room and Power-link).

IS Security knowledge is also stored within entities such as **organisational units**, the organisation itself and inter-organisational networks. The firm stores specific knowledge regarding: the norms, values, practices and culture which embody the organisation. The knowledge stored in units, such as a department represent the formal functions of individual stores of knowledge specific to a unit or function (Huang et al., 2007). CME-Co and TELE-Co used customer feedback as a guide or measure for productivity and as a source of market demand. However CME-Co established a group specifically to target IS Security stakeholders. Security Officers, as groups, coordinate the roll-out of controls across the subsidiaries and collaborate on activities such as audits and in conducting post-mortems. Thus, the two organisations established KM communities of practice which were function specific. Knowledge transfer has extended from passing information from individual to individual (Cantoni et al., 2001) to moving knowledge around the organisation (Rutkowski, 1999). As a result the collective

knowledge of a function is synergistic (Becerra-Fernandez et al., 2004). Conversely while TELE-Co's utilisation is internally focussed, CME-Co pushed knowledge towards customers and partners to create additional knowledge and reduce cost through the utilisation of a knowledge self-help reservoir.

Knowledge is also stored in **inter-organisational relationships** such as collaborative partnerships. Vendors were used to provide guidelines, product and technological specifications. The inter-relationships were formed to exploit financial opportunities. CME-Co established and utilised a Corporate Security group to analyse the security industry and identify stakeholder requirements. TELE-Co has hosted IS Security and CS symposiums to identify the direction of regulatory and market requirements. CME-Co enhanced their inter-organisational relationships through the use of collaborative forums such as Power-Link and E-Room. The two organisations exploited inter-organisational relationships to acquire market and regulatory knowledge and to ultimately manipulate the environments the organisations operate in. While the importance of collaboration between organisations is reported in the literature (Dutta & McCrohan, 2002), the advantage of steering the market as not reported (Stewart, 2005).

Figure 7.3 presents a synthesised representation of the different reservoirs of IS Security knowledge an organisation should utilise. The different levels of expertise are viewed as a significant source of knowledge within the two organisations. CME-Co created ad hoc knowledge development groups and coordinators to develop lower level support skill-sets and ensure solution standards. Procedures such as solution templates and management techniques are viewed as important sources of knowledge. CME-Co's and TELE-Co's internal and external documentation was sourced to comply with corporate requirements, particularly in documenting lessons-learned and case solutions. Knowledge tools, repositories and email were used to store knowledge. It is also evident that both organisations are dependent on inter-relationships with external evaluators for IS Security. However CS knowledge stores were primarily internal to the functions. CS knowledge was focussed on the organisations product portfolios. Therefore internal sources of knowledge were vital. The reporting structures used, highlighted IS Security's structural and financial importance to the two organisations. This ensured that IS Security had political support at senior levels particularly in relation to regulatory drivers and evaluations. Finally formal groupings were also established, in the two organisations, to focus on regulatory issues. However CME-Co used the opportunity to create a group to identify stakeholder requirements. As a result the IS Security functions are dependent on external sources of knowledge.

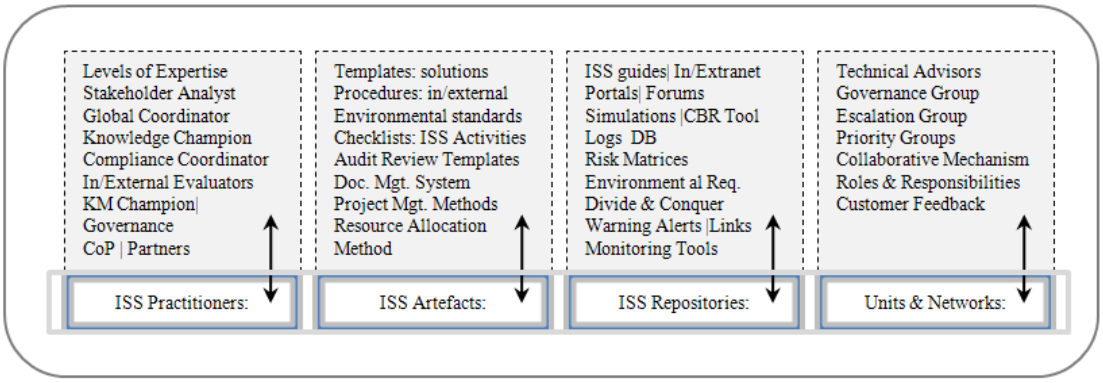

Figure 7.3: IS Security Reservoirs

7.2.3 Interpreting the IS Security Knowledge Processes used in the Case Studies

The objective of most organisations, attempting to manage knowledge regardless of the type, is to capture, share, acquire, use, control and create explicit and tacit knowledge (Standards Australia, 2001). The ISS knowledge processes identified in the CME-Co and TELE-Co case organisations are described and compared in the following sub-sections.

(1) Knowledge **acquisition** is the process by which knowledge was obtained and transformed into a representation that was internalised by CME-Co and TELE-Co (Appendix E & Appendix G: Rows 1). Tables 5.1 and 6.1 broadly outline the tendency of the two organisations to acquire external knowledge. CME-Co was inclined to purchase companies to enhance its product portfolio (rapid remote) and enhance its inter-organisational relationships through collaborative software (E-Room). However the acquisition of knowledge by TELE-Co is not common. Table 6.1 illustrated a propensity to sell companies, diversify, enter new markets, innovate with first to market products, create methodologies and quality mechanisms (acquired by other leading multinationals). Therefore the multinationals, at firm level, utilised two different approaches in acquiring external knowledge resulting in or due to profit inclines and declines. The two organisations, at functional levels, used acquired software to collaborate, techniques such as reverse-engineering to innovate, and IS Security standards to adhere to industrial best practices. Subscription to external technical communities of practice and vendor repositories was fundamental in acquiring new security technologies, manuals and best practices. Additionally, active membership of regulatory bodies, by CME-Co and TELE-Co, allowed the organisations to determine the steps taken by other companies in auditing, reviews and the expected direction of the industry. As a result the two organisations have participated in driving their respective markets to stay ahead of their competitors and mould their regulatory environments. Best practices, regulatory guidelines, and standards were purchased and customised, by the IS Security functions, to comply with U.S. and international regulatory laws. External auditors and security specialists were hired to avail of their testing and auditing expertise.

Training courses were purchased, customised and delivered through Knowledge-Link by CME-Co. However, the two organisations used simulations to train new CS Technicians for fire-fighting in CME-Co (lab simulations) and for product development in TELE-Co (CAD). Corporate and competitor products were acquired and used, by the two organisations, in developing reverse-engineering and diagnostic skill-sets. The practice provided knowledge for training, in interoperability problem-solving, product enhancement and competitor analysis. The two organisations have collaborated with academia and industry through collaborative forums such as the ISF and conferences. However TELE-Co has facilitated the collaboration of academics and other organisations through a yearly TELE-Co symposium. This platform enabled the organisation to determine the direction of, for example, new simulation software and to in effect direct the market. Therefore the two organisations have sourced external knowledge to comply with environmental regulatory constraints and to stay ahead of market developments and their competitors.

(2) The IS Security and CS functions **captured** knowledge from the CME-Co (Appendix D) and TELE-Co (Appendix F) reservoirs (Appendix E & Appendix G: Rows 1). The two organisations utilised a pool of experts or practitioners in problem-solving. The roles and responsibilities assigned to individual members of the

organisations aided the identification of experts located across the multinationals. Technological mechanisms such as email and portals enabled the organisations to pull knowledge in order to facilitate collaboration, the creation, sharing, and storage of solutions. Central repositories (Channel CME-Co and Compass) were identified as the primary tools used to retrieve manuals, documentation and procedures. The IS Security functions used external evaluators to conduct evaluations in preparation for audits to test the level of security within the organisation, through network vulnerability testing. This is an ongoing review process requiring the documentation and adoption of lessons-learned from one review to the next. However the CS functions used technological mechanisms to capture knowledge. CME-Co's CS function used the case-based reasoning tool (Primus) to capture, create, share, store and reuse solutions pertaining to the CME-Co product portfolio. TELE-Co's CS function used simulation models and software to design and test data across design domains. The CME-Co CBR tool facilitated external collaboration (Power-Link). Customers and partners have retrieved existing solutions and created new solutions. Therefore CME-Co has captured and reused partner knowledge in problem-solving. This self-service programme and platform enabled partners and customers to solve their own problems and reduce CME-Co costs and increase CS productivity.

(3) The two organisations **created** solutions through problem-solving (Appendix E & Appendix G: Rows 3). Lessons-learned were documented due to the utilisation of the M-Gates project management methodology and IS Security audits. Mechanisms were used by the IS Security functions to facilitate the creation of new IS Security and CS knowledge. The Portfolio Project Management (PPMG) group identified the security requirements of other business functions within CME-Co. TELE-Co utilised methodologies (M-Gates) to coordinate a collaborative approach to problem-solving. Documents such as the SRD and risk assessment techniques were used to determine security requirements and identify security product enhancements. The evaluation and resulting documentation of audit reviews and lessons-learned were environmentally driven. CS identified the potential of leveraging the knowledge of CME-Co partners and vendors in creating and sharing new solutions (knowledge) to reduce costs. The CS functions operating within CME-Co and TELE-Co created solutions using the different levels of support (escalation process). CME-Co's partners were used extensively to create and share solutions in order to reduce costs. TELE-Co created design solutions through the utilisation of simulation software and the M-Gates methodology. Solutions were not shared with partners but function specific. The IS Security functions created and acquired evaluation reports (audit reviews), identified security controls, customised standards and best practices for compliance deliverables. Mechanisms such as brainstorming (enabled through online forums and teleconferences) were used to conduct post-mortems of activities such as audits. The IS Security functions utilised a trial and error approach in allocating controls in TELE-Co and CME-Co. Individual members were granted access to corporate resources based on their organisational roles and responsibilities in enforcing segregation of duties. The IS Security functions reassessed access rights when additional requirements were identified. Lessons-learned and audit documentation were created and used to improve internal and cross-functional processes.

(4) The IS Security and CS functions **shared** knowledge through the utilisation of tools such as email, teleconferences and collaborative platforms (Appendix E & Appendix G: Rows 4). However CME-Co utilised a CBR tool and TELE-Co utilised a central repository to share knowledge internally and symposiums to share knowledge publicly. The two organisations generated and shared knowledge through their problem-

solving escalation processes. Knowledge trading was identified in CME-Co and TELE-Co. Help, in the form of an (ISS or CS) practitioner or a document was often traded to ensure collaboration at a later date. CME-Co collaborated extensively with customers and partners in sharing solutions to reduce support costs and increase the productivity of the CS function. Regulatory bodies were used to participate in the creation and sharing of standards and to drive the market. The IS Security functions used coordinators and mechanisms (PPMG and SRD) to encourage the collaboration and sharing of knowledge across functions and subsidiaries. IS Security practices were shared externally through forums to learn from and collaborate with other organisations in sharing lessons-learned and in steering the security industry. CS shared product designs, solutions and test data internally in TELE-Co and increasingly with partners in CME-Co. Therefore, the difference between the organisations approaches to sharing is functional. IS Security will search for and collaborate with partners to steer the security market and CS will push or drive solution knowledge across the different design domains in TELE-Co and towards customers or partners in CME-Co.

(5) Knowledge **application** involved the use of knowledge in guiding decisions and actions (Appendix E & Appendix G: Rows 5). The two organisations created, used, customised and stored knowledge in the form of solutions, standards, and best practices. Pools of IS Security and CS practitioners were used to collaborate, share and therefore use and reuse knowledge in problem-solving and decision-making. The IS Security functions utilised security technologies to build pictures of the CME-Co and TELE-Co security landscapes. Standards and best practices were purchased customised and reused. Audit reviews were used to improve practices as lessons-learned were documented. The IS Security functions exploited the auditing process to apply and reuse knowledge from past reviews as benchmarks for forthcoming reviews. However TELE-Co's CS function utilised the M-Gates methodology to apply the knowledge generated at each gate. Simulation software enabled the function to build prototypes and collaborate across the different design domains. CME-Co's CS function utilised a CBR tool to efficiently store, share, retrieve and reuse solutions. Experienced Engineers were used to integrate knowledge manually as reverse-engineering and diagnostic skills cannot be replicated by the technologies used in either organisation. The application of IS Security and CS knowledge across the functions was very different. IS Security purchased customised and reused external knowledge. Lessons-learned were documented through post-mortems and external measures or processes were used to improve internal activities. The CS functions required the use of project management methodologies and tools to enable the coordinated reuse of knowledge. As a result knowledge was pulled from different sources. The IS Security functions purchased and customised external knowledge to adhere to environmental requirements and CS created knowledge internally.

(6) Knowledge **control** secured valuable functional and therefore corporate knowledge (Appendix E & Appendix G: Rows 6). The two organisations used focused IS Security strategies in protecting their corporate boundaries. IS Security was divided, in the two organisations, structurally to focus on its different security facets. Groups targeted external environmental requirements to adhere to regulations and internally for controlling dispersed organisations. Security technologies were used to control and protect resources. Systems (assets) were prioritised according to their value and controls aligned were aligned as required. Organisational resources such as repositories, product designs and Engineering labs were allocated controls in order to protect the innovative processes and the innovators themselves. Controls were extensively allocated to documents to ensure quality, utility, consistency and ownership. However CS, and

particularly Engineering, was regarded by senior management as innovators who required complete control over their systems and networks. Engineering applied controls, such as access rights, to their own systems. The two organisations used formal, informal and technical controls to control the behaviour of unauthorised users. Additionally the two organisations utilised tools and mechanisms to monitor and track internal traffic in order to identify rogue behaviour. Virtual private networks were used to encrypt the communication lines and legal documents, such as NDAs, were used to control employee behaviour.

The next section describes the IS Security KM processes identified and then compared to the literature.

7.2.3.1 IS Security KM Processes

Knowledge Management (KM) is concerned with ensuring that knowledge is available in the right form to the right processors (systems, people and processes) at the right time for the right cost (Holsapple & Singh, p.220).

Knowledge acquisition is the process by which knowledge is obtained (Huber, 1991, p.90). Once it is identified it is transformed into a representation that can be internalised (Holsapple & Singh, 2004). CME-Co was inclined to purchase companies to enhance its product portfolio and enhance its inter-organisational relationships. However the acquisition of knowledge by TELE-Co was not common. The multinationals, at firm level, utilised two different approaches in acquiring external knowledge. The two organisations, at functional levels, used acquired software to collaborate, techniques to innovate, and IS Security standards to adhere to industrial best practices. Subscription to external technical communities of practice and vendor repositories was fundamental in acquiring new security technologies, manuals and best practices as advocated by Stewart (2005). Active membership of regulatory bodies, by CME-Co and TELE-Co, allowed the organisations to determine the steps taken by other companies in auditing, reviews and the expected direction of the industry (Stunt, 2006). The two organisations have participated in driving their respective markets to stay ahead of their competitors and mould their regulatory environments. Training courses were purchased, customised and delivered through the corporate universities. Corporate and competitor products were acquired and used in developing reverse-engineering and diagnostic skill-sets (Becerra-Fernandez et al., 2004). As a result the two organisations have sourced external knowledge to comply with environmental regulatory constraints and to stay ahead of market developments and their competitors.

The IS Security and CS functions **captured knowledge** from the corporate reservoirs as described in the literature (Becerra-Fernandez et al., 2004).. The two organisations utilised a pool of experts or practitioners in problem-solving. The roles and responsibilities assigned to individual members of the organisations aided the identification of experts located across the multinationals (Eppler, 2004). Technological mechanisms such as email and portals enabled the organisations to pull knowledge in order to facilitate collaboration, the creation, sharing, and storage of solutions. Central repositories were identified as the primary tools used to retrieve manuals, documentation and procedures. The CME-Co CBR tool facilitated external collaboration (Power-Link). Customers and partners have retrieved existing solutions and created new solutions. Therefore CME-Co has captured and reused partner knowledge through problem-solving (Nonaka, 1994).

Knowledge creation is a sign of a healthy organisation becoming a learning organisation (Coakes, 2004), arguing that knowledge does not remain static as in either of the two case organisations. Leveraging tacit knowledge is a difficult process and central to its attainment is the collaboration of the actors (Hislop, 2005). The IS Security and CS functions captured knowledge from the CME-Co and TELE-Co knowledge reservoirs. The two organisations utilised a pool of experts or practitioners in problem-solving. Central repositories (Channel CME-Co and Compass) were identified as the primary tools used to retrieve manuals, documentation and procedures. The IS Security functions used external evaluators for ongoing review processes requiring the documentation and adoption of lessons-learned, which was not reported in the literature. The CME-Co CBR tool facilitated external collaboration (Power-Link). To facilitate these processes the structure, management and the necessary ICT must support them. There are four modes of knowledge conversion required for knowledge creation: (1) socialisation, (2) externalisation, (3) conversion and (4) internalisation as identified by Nonaka et al., (1996) and replicated across the two organisations.

1. **Socialisation** is the process by which tacit knowledge from one individual is converted into the tacit knowledge of another though observation and practice. CME-Co and TELE-Co both used: trial and error learning, on the job training, mentoring, direct or indirect communication.
2. **Externalisation** is the process of changing tacit knowledge into explicit through dialogue and group reflection. The review process for audits forced both ISS functions to document the lessons learned for each review.
3. **Combination** is a process of combining components of explicit knowledge to create and store in knowledge systems such as: KMS, databases and documentation, enabling additional members of the unit or organisation to access knowledge. CME-Co was an active advocate of combining explicit knowledge through Primus. TELE-Co was very much dependent on the skills of its Engineers to combine design knowledge.
4. **Internalisation** is the process through which experts can personalise explicit knowledge and convert it into tacit knowledge. The two organisations were active in internalising knowledge. However while CME-Co was active in doing so both internally and externally. TELE-Co was domain specific

Pools of IS Security and CS practitioners were used to collaborate, share and therefore use and reuse knowledge in problem-solving and decision-making. **Knowledge sharing** is the process through which explicit or tacit knowledge is communicated between individuals, groups, units or organisations. The IS Security and CS functions in TELE-Co and CME-Co shared knowledge through the utilisation of tools such as email, teleconferences and collaborative platforms. However CME-Co utilised a CBR tool and TELE-Co utilised a central repository to share knowledge internally and symposiums to share knowledge publicly. Regulatory bodies were used to participate in the creation and sharing of standards and to drive the market, a fact not identified in the literature. However, as reported, the two organisations created informal (TELE-Co) and formal (CME-Co) communities where knowledge was shared and used by developing CoP (Pan & Leidner, 2003).

Knowledge application involves the use of knowledge to guide decisions and actions. ISS knowledge was used and applied by the two case organisations which, as a result, facilitated organisational learning and therefore provided indirect and direct value to the organisations (Holsapple & Joshi, 2004; Jashapara, 2004). The organisations created, used, customised and stored knowledge in the form of solutions, standards, and best

practices. The IS Security functions utilised security technologies to build pictures of the CME-Co and TELE-Co security landscapes as identified as vital by Booz et al., (2005), Baskerville, (2004) and Dhillon (2006). Lessons-learned were documented through post-mortems and external measures or processes were used to improve internal activities. These processes were however not identified in the literature as value added activities.

Finally, the two case organisations availed of IS Security strategies to protect their corporate boundaries. Groups targeted external environmental requirements to adhere to regulations and internally for controlling dispersed organisations. To protect information or knowledge assets, management allocated, as advocated in literature, appropriate IS Security and **knowledge control** measures to counter known threats (Jamieson & Handzic, 2004; Becerra-Fernandez et al., 2004; CSI, 2009). Security technologies were used to control and protect resources. Systems (assets) were prioritised according to their value and controls aligned were aligned as required (Jamieson & Handzic, 2004). Organisational resources such as repositories, product designs and Engineering labs were allocated controls in order to protect the innovative processes and the innovators themselves. Control is a managerial influence on KM to assure knowledge validity (accuracy and consistency) and knowledge utility (relevance and importance), (Jamieson & Handzic, 2004; Holsapple & Singh, 2004). The two organisations used formal, informal and technical controls to control the behaviour of unauthorised users. Knowledge control should be a priority as the value of knowledge and the returns achieved depend on the effectiveness of the controls (IT Governance Institute, 2001; Randeree, 2006). However, ISS viewed KM as a project and allocated controls as they would to any new system or process.

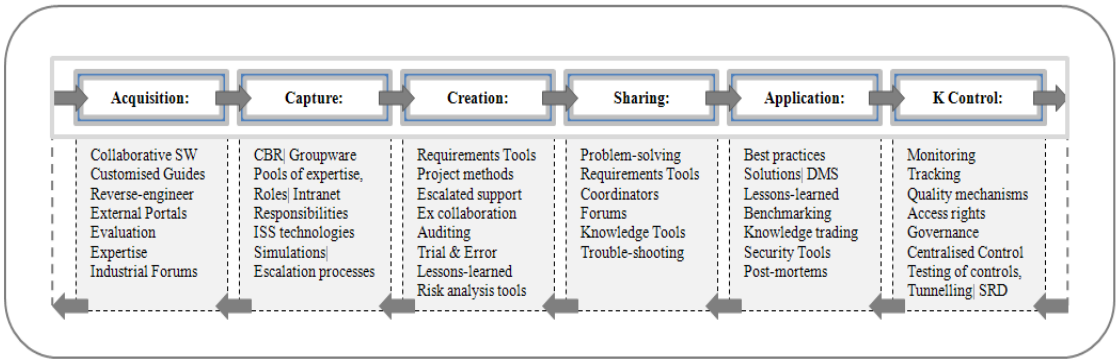

Figure 7.4: IS Security Processes

Figure 7.4 presents a synthesised representation of the different types of IS Security knowledge processed. A significant amount of knowledge was acquired externally by CME-Co. Collaborative software, regulatory guidelines, subscriptions, products and external evaluations were acquired by the functions to ensure that the two case organisations are compliant within their business environment and aware of any and all business opportunities such as market changes and competitor product advancements. Problem-solving was the principal approach used to create knowledge and applied through the reuse of the solutions created and stored. The CME-Co and TELE-Co IS Security functions purchased significantly more external knowledge than CS due to regulatory requirements. This environmental driver enabled the IS Security functions to exploit the auditing process and use reviews as benchmarking aids in applying lessons-learned to internal and external IS Security activities. Problem-solving was identified in the two organisations as the principal approach used to create knowledge and applied through the reuse of the solutions created.

7.2.4 Interpreting the IS Security KM Mechanisms used in the Case Studies

This section describes the **mechanisms** used in CME-Co and TELE-Co to promote the management of IS Security knowledge. Table 7.3 (adapted from Tables 5.11 and 6.11) outlines the mechanisms which are divided by type, and illustrates which are common or unique to the two case organisations (√√).

Table 7.3 illustrates the high volume of KM mechanisms used in the two case organisations. It is evident that the IS Security functions utilised formalised mechanisms and external measures compared to the CS utilisation of ad hoc mechanisms utilised to drive KM within the two organisations. The support functions within TELE-Co and CME-Co utilised the different learning mechanisms. This varied according to budget or if specific training (SETA) was required. Collaborative mechanisms such as: brainstorming, problem-solving and face-to-face meetings were used by the TELE-Co and CME-Co's CS and IS Security functions. DMS were used unless a corporate specific procedure (POPI) was required. Formal groups or structures were used by the IS Security functions which were aligned to the CME-Co and TELE-Co strategies. The two organisations implemented KM as an ad hoc initiative. Internal collaborative tools were exploited by the two organisations across the IS Security and CS functions. Public forums were used by the two organisations but to varying degrees. The problem-solving tools identified were specific to the functions. Simulation software was used by the CS functions for decision-making and training.

Finally, the monitoring and tracking tools were used by the IS Security functions. The significant difference between the two organisations and functions was the utilisation of a case based reasoning tool. CME-Co positioned its CS knowledge management initiative around Primus. Due to the dedication of CS practitioners the role of the tool was gradually increased as its value to CME-Co was continuously demonstrated to the different levels of support and to senior management. Additionally, Primus was used to provide CS solutions to and as a self-service support environment for CME-Co customers and partners. CS utilised quality mechanisms for the solutions created, allowed knowledge filtering, advanced search criteria's and pushed CS knowledge towards CME-Co customers. Therefore the IS Security functions were externally driven to comply with specific goals and measured due to regulatory requirements. CME-Co's CS function was driven to develop skills and utilise practitioner knowledge more efficiently. TELE-Co positioned its KM initiative around M-Gates and PKM for specific design domains as opposed to the entire CS function. IS Security utilised KM mechanisms to support the organisational goal of protecting the corporate assets, adhering to regulatory constraints and sourcing environmental opportunities for exploiting potential markets.

7.2.4.1 Functional IS Security KM Mechanisms

In the literature mechanisms are categorised as either technological or non-technological. However the mechanisms identified in the two organisations were further categorised according to their objectives to determine their use. They were supported by the KM organisational infrastructure and facilitated by KM systems (Becerra-Fernandez et al., 2004). KM mechanisms identified ranged from on-the-job training, learning by training, face-to-face meetings, mentoring, employee shadowing, employee rotation, brainstorming and analogies. While only on-the-job-training/learning and a face-to-face meetings were regarded as formal mechanisms in TELE-Co and CME-Co, mentoring, employee shadowing/rotation and brainstorming varied and were utilised on an informal

basis. Mechanisms which facilitated socialisation in the two case organisations included: cooperative projects across departments, repositories of best practices, and lessons-learned. However apprenticeships were not utilised due to, primarily, to budget constraints. Cooperative projects were utilised and formalised through methodologies and checklists Dhillon, 2006).

	KM MECHANISMS		CME-Co		TELE-Co	
			ISS	CS	ISS	CS
Non Technological	**Learning | Training KM Mechanisms:**					
	Induction Training:	Specialised for the different functions	√	√	√	√
	Learning on the Job:	Responsibilities are added gradually	√	√	√	√
	Analogies:	Stories describing the competitive nature of Org.	√	√		
	SETA:	Penalties for Breaking Security Procedures	√		√	
	Mentoring:	Provide Access to Experts	√	√	√	√
	Lab Simulations	Learning environment for problem-solving		√		√
	Job Rotation	Learning		√		
	Reviews:	6 month Assessment of Employees			√	√
	Corp. University	Up-skill to meet Specific Needs	√	√	√	√
	Collaborative Sessions:					
	Teleconferences:	Used for Global Communication	√		√	√
	Minutes of Meetings	Recorded & Stored			√	√
	Meetings:	Face-to-Face	√	√	√	√
	Brain Storming	Audit Reviews	√	√	√	√
	Problem-solving	Collaborative Process	√	√	√	√
	Documentation Quality Systems & Procedures:					
	SRD:	Aligning Security Requirements			√	
	DMS:	Doc. Templates & Quality Procedures	√	√	√	√
	Prj. Mgt. Method	Phased approach to managing projects	√			√
	Business Case	Project Resources & ID Roles Responsibilities	√	√	√	√
	Individual & Groups of Expertise:					
	Expert Status:	Expertise List	√		√	√
	Global ISS Group	Global Security Group: Coordinate Teams	√		√	
	Global IP	Global Compliance Group	√		√	
	KM Team	Promote KM		√		√
	KM Roles	KM Leadership		√		√
	Symposia	Collaborate with Industry & Academia			√	√
KM Tools	**Internal Collaborative Tools**					
	Intranet:	Central Document Repository & Group Resource	√	√	√	√
	CMS:	Stores Lessons-learned, Document Store	√	√	√	√
	Groupware:	Collaborating & Sharing Solutions	√	√	√	√
	Hyperlinks	Links to Internal & External Solutions	√	√	√	√
	Common Shares	Groups, Regional Shares, Stores Procedures	√	√	√	√
	Public Forums					
	Vendor Portals	Procedures, Guidelines and Best Practices	√	√	√	√
	Forums	Public Collaboration	√	√	√	√
	Problem-solving Tools					
	CBR	Case-based Reasoning Tools		√	√	√
	Simulation Models	System & Paper-based for Product Components		√		√
	CAD Tools:	Computer Aided Design for Product Simulations		√		√
	MS Excel:	Risk Matrixes, to calculate the level of risk	√		√	
	Monitoring & Tracking Tools					
	ART:	Automated Analysis, Reporting Tracking Tool	√		√	
	Scanning SW:	Monitors Rogues & Internal Employees	√		√	
	VPN:	Tunnelling to Protect Communication NWs	√		√	
	Wireless Tech.	2-way Pagers from Systems or Call logging System	√	√	√	√
***Organisational Level:** √√ *** Specific to One Function:** √						

Table 7.3: CME-Co and TELE-Co KM Mechanisms Used by the IS Security and CS Functions

The two organisations combined their knowledge through the collaboration of documentation (solution templates), databases (vendor), problem-solving methodologies and web-based access to data through Primus and Compass. However CEM-Co utilised external partner knowledge to a greater extent through PowerLink. Knowledge capture was facilitated by case-based reasoning tool –Primus in CME-Co. TELE-Co utilised Compass purely as a central repository as opposed to a true KMS (Butler & Murphy, 2007). Knowledge sharing was facilitated through corporate repositories, lessons-learned were documented by both case organisations but purely to adhere to compliance requirement. Expertise locators were not used by either organisation, contrary to the advantage reported in the literature (Eppler, 2004) personal contact lists were used instead. Support centres were used to facilitate direction, and policies and standards are used to support routines in CME-Co and TELE-Co as advocated by Becerra-Fernandez et al., (2004).

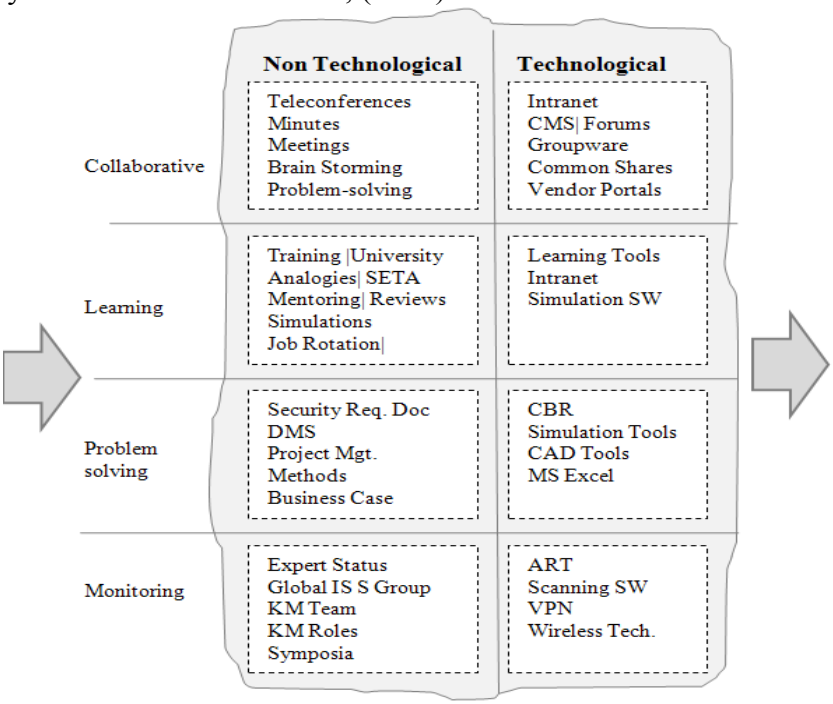

Figure 7.5: IS Security Mechanisms

Figure 7.5 presents a synthesised representation of the different types of IS Security KM mechanisms an organisation should utilise. The typical goal of a KM initiative is to capture knowledge in a documented form and store it into a repository where it can be easily stored and retrieved by knowledge workers (Davenport & Prusak, 1998). While TELE-Co attempted to do this through Compass. It was regarded by the interviewees as a DMS. However CME-Co pushed knowledge sharing and use internally and externally through its CBR tool. This enabled the combination and integration (Nonaka, 1994) of knowledge, along with the capability to combine an expert's experience in the form of a system to provide a strategic tool (Alavi & Leidner, 2001) for the CS function in CME-Co. However this advantage was very much function specific. The technological mechanisms used by the case organisations were capable of combining explicit and tacit knowledge of workers to varying degrees (Butler & Murphy, 2007). These systems were used to acquire and manage knowledge and distribute it among the CS and ISS functional units as well as with any external collaborating functions in CME-Co to create new knowledge through the use of the different mechanisms (Alavi & Leidner, 2001) and therefore improving the effectiveness of decisions (Peterson, 1996).

7.2.5 Interpreting IS Security KM Impacts in the Case Organisations

This section describes the impact of managing IS Security knowledge within CEM-Co and TELE-Co. While the IS Security functions did not utilise a knowledge management strategy, the ISS functions within TELE-Co and CME-Co, as a result of regulatory requirements, managed their knowledge.

The IS Security and CS practitioners within the two case organisations did learn new skills and attend collaborative conferences. TELE-Co ISS practitioners did have access to training, conferences, and were regularly reviewed. TELE-Co and CEM-Co provided the functions with the tools needed to tackle complex problems. ISS knowledge was shared across the different functions to ensure each organisation was secured. Therefore, compliance has positively impacted the individual ISS practitioner. CME-Co's CBR tool - Primus had a very positive impact on CS practitioners. The CBR tool reduced the time needed for training, facilitated the creation of solutions for a complex product portfolio. Knowledge sharing has also been significantly increased with escalated levels of support for the two case organisations.

The two IS Security functions are externally reviewed. Knowledge tools were used to centralise IS Security knowledge and problem-solving was coordinated. As a result, the ISS role became easier due to the utilisation of externally tested processes and practices. Specialised IS Security groups coordinated and shared knowledge across the two organisations. Audits provided measurements and facilitated learning through post-mortems forcing a proactive stance against IS Security challenges. CS practitioners utilised prototyping to facilitate learning in addition to corporate training. Symposiums allowed the CS function to collaborate with other organisations and academics. KM tools (such as Compass) retained individual knowledge for reuse. Development standards and templates ensured easy collaboration across the functions and organisations. The IS Security and CS functions benefited from the individual impact of the management of IS Security and CS knowledge in CME-Co and TELE-Co. Best practices and standards for managing security were sourced and implemented to provide greater organisational security. Solutions created were stored and reused which reduced the amount of time needed to solve problems. Audits forced the recording of lessons-learned and generated significant knowledge for future audits. CS utilised escalation processes and reverse-engineering skills to increase CS knowledge in the two organisations. This ultimately increased productivity and enabled product enhancements. CME-Co's CBR tool reduced costs and enhanced the organisations relationship with its customers through the introduction of a (customer or partner) self-service portal.

External evaluators measured the IS Security functions activities and provided useful feedback for improvements. CME-Co's CS function utilised a significant volume of external sources of knowledge in order to remain as industrial and environmentally aware as possible. Best IS Security practices and standards were sought. TELE-Co and CME-Co were evaluated to improve security internally. The auditing process also had positive impacts for the two IS Security functions. It forced the practitioners to undertake post-mortems at the end of a review which enhanced learning. Auditing has resulted in significant improvements in TELE-Co and CME-Co. Processes were documented and knowledge regarding the organisations security status was constantly pulled from internal and external knowledge reservoirs. The efficiency of the IS Security processes were measured by determining the number of calls from customers and the number of improvements made as a result of an audit. CS processes were

enhanced through employee rotation (on an ad hoc basis), brainstorming sessions and the recognition of practitioner contribution to the CBR tool. The number of solutions hits were measured and rated to create a competitive culture within CME-Co's CS function. Processes were also evaluated through the improvements made. TELE-Co exploited standardised templates and procedures to alleviate IS Security workloads. Reviews were used to guide the next audit and are ongoing evaluations of the IS Security functions. Reverse-engineering and diagnostic skills provided valuable competitive knowledge for the two organisations. Escalation processes enabled improved services and products for customers and faster response time for fixes. However knowledge was domain specific in TELE-Co which provided an advantage to the design domains availing of the strategy. Solutions for problems or designs were not made available to Customers or to some domains as was reported in CME-Co.

7.2.5.1 IS Security KM Impacts

Malhorta (2003, p.3) contends that "…knowledge has no definitive value but can potentially be of use indefinitely." Even though knowledge was difficult to quantify in the two case organisations it was a significant component of the decision-making processes illustrated and discussed in this chapter. It did have a clear impact on the business outcomes of the two case organisations (Soo et al., 2002). Intangible assets such as knowledge added services were difficult to appraise in TELE-Co and CME-Co but researchers have argued that they should not be ignored (Conway, 2004; Ulrich & Smallwood, 2004) as they provide numerous benefits (Tables 5.12 and 6.12). Brelade and Harman (2003) argued that the drivers for KM are much the same as drivers for change in any organisation; to obtain a competitive advantage. TELE-Co and CME-Co utilised knowledge management, in their CS functions, to achieve a competitive advantage. However, it was CME-Co which consistently pushed the use of the strategy to identify additional advantages in order to more effectively compete. TELE-Co's use was very much domain (or CoP) specific despite obvious advantages. As the majority of organisations regard the knowledge possessed by the firm as an asset, particularly regarding expertise. Therefore, it was the management, creation and application of this knowledge in CME-Co that was a direct contributor in achieving and maintaining a sustainable competitive advantage as identified by Stewart (1997). The CS and Engineering practitioners through the implementation of the KM initiatives in TELE-Co and CME-Co made more effective decisions, improved their efficiency and in turn improved the profitability of the two case organisations through the effective management of knowledge (Coakes, 2004).

CME-Co placed an emphasis on knowledge, skills and creativity and on the capturing and sharing of information through the creation of knowledge roles (knowledge champions): solution quality reviews (KCS), formalised communities of practice (KDG) and the use of a CBR tool. These are all issues that impact upon how people are managed (Brelade & Harman, 2003). Alternatively, TELE-Co did not support the initiative at a senior level and it was advocated at a domain level through an informal community of practice (PKM). However the two organisations showed evidence of knowledge hoarding between Engineering and the other corporate functions. Engineers hoarded their knowledge rather than share it. Unless knowledge sharing is rewarded more than knowledge hoarding (Davenport & Prusak 1998; Walsham 2001) practitioners will continue to hoard. The dilemma for knowledge workers is that there are potentially positive and negative consequences to both sharing and hoarding knowledge. The advantages of sharing knowledge maybe rewarding, with benefits at the group level (increased performance) which was evident in the ISS functions and at the

organisational level, and an individual's status maybe enhanced as it was in the CME-Co CS function. The negative implications vary from loss of power as indicated by the Engineering functions and time as reported by all of the interviewees in the two case organisations. Moreover, knowledge sharing is dependent on the motivational elements of the knowledge sharing process and the culture in which the process operates. However it is interesting that the ISS functions in the two case organisations were as positively impacted by managing knowledge as the CS functions which purposefully utilised a KM initiative. Therefore, as reported by Raghu and Vinze (2005), it is possible for knowledge sharing to be successful even without a set structure for knowledge sharing, as long as there is a context for knowledge initiative. In the context of this investigation compliance, unexpectedly, forced the ISS functions to manage ISS knowledge.

A general weakness of KM initiatives is that the issues of conflict, power and politics are generally neglected (Hislop, 2005). CME-Co's and TELE-Co's management of ISS knowledge was facilitated through the requirements of regulatory adherence and the necessary approaches to managing ISS knowledge and structural changes (ISS senior role) were made. However the potential for conflict between workers and management can shape individuals willingness to participate in organisational knowledge processes. Engineering groups could bypass any initiative to access their knowledge even a managerial decision. Therefore inter-personal and inter-group conflict in the organisations can also affect KM processes (Hislop, 2003). This was, as explained in CME-Co, a direct result of a history of inter-functional conflict and competition between CS and Engineering. ISS regarded the power utilised by Engineering as disruptive yet unavoidable. TELE-Co management ignored the conflict so that the innovative creativity of Engineering would not be interfered with. Furthermore, knowledge and personal networks were used by many practitioners in CME-Co and TELE-Co as political tools in support of particular objectives (Hislop et al., 2000) in trying to access functional knowledge (Buchanan & Gibb, 2008). However the importance of conflict, power and politics in impacting workers willingness to share is profound. They are a common feature of organisational life and due to the inter-relationship between power and knowledge, knowledge is a resource workers make use of in dealing with situations of conflict, as evident in the Engineering functions of the two case organisations.

Figure 7.6 presents a synthesised representation of the different types of impacts an organisation should achieve through the utilisation of a KM initiative. Employee performance can be greatly impacted through KM or another initiative which facilitates knowledge sharing. In the case of this investigation compliance forced the management of ISS knowledge in the two case organisations. It facilitated ISS and CS individual learning and enhanced their exposure to the latest knowledge in their fields of expertise through for example access to experts and lessons-learned from one audit to another. Employees were also encouraged to learn from one another to adapt to inter-operability changes in their environments. These improvements also enhanced job satisfaction as skills were improved, as is the employee's market value (Brown & Duguid, 1991). Additionally KM facilitated improvements in organisational processes by improving the effectiveness, efficiency and innovativeness of the different processes to varying degrees across the two organisations. Specifically KM enables organisations and their functions to adapt quickly to changes in their environments, such as the IS Security landscape and technological advancements.

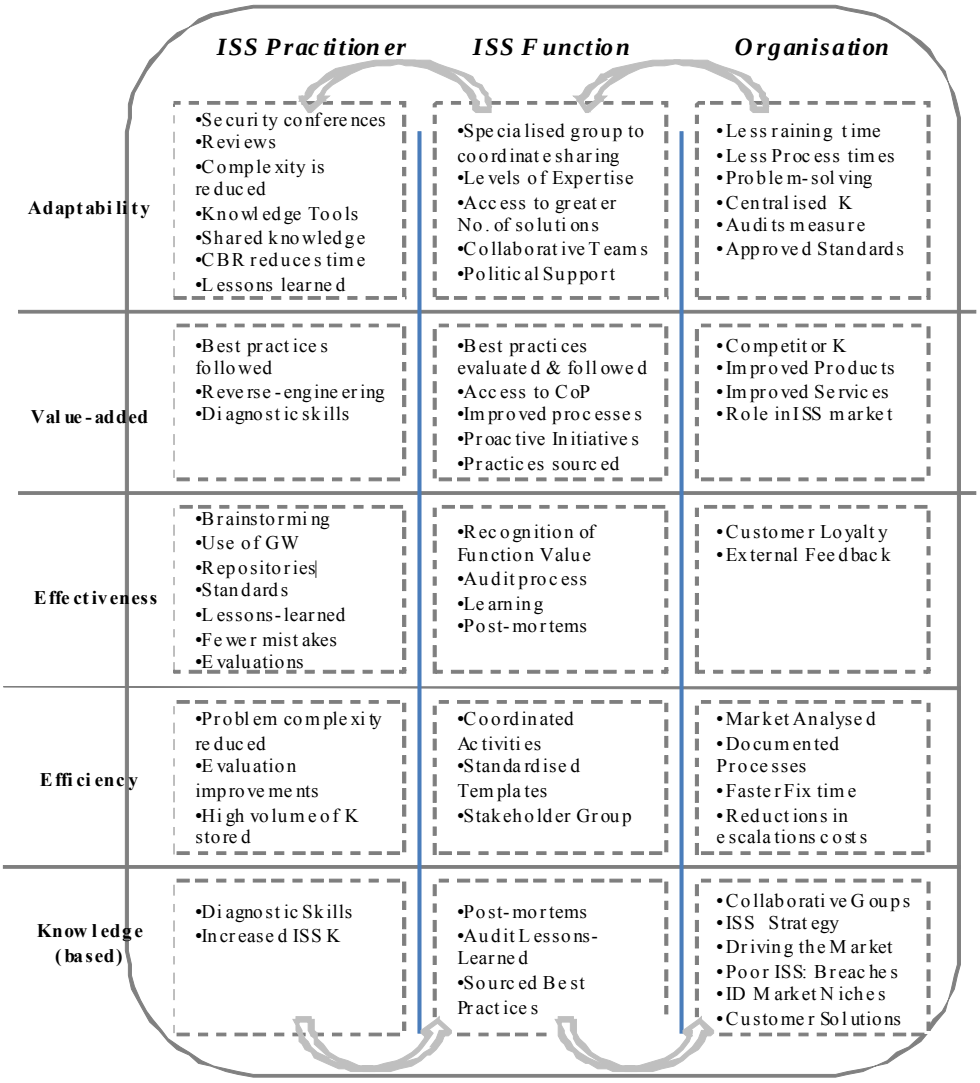

Figure 7.6: IS Security Impacts

CME-Co was much more innovative in its approach to utilising internal and external knowledge than TELE-Co. Both companies did improve their corporate products and services through KM (Choi & Lee, 2002). Essentially existing products were improved to add value to the organisation, and the knowledge-intensive services: CS and ISS within CME-Co and TELE-Co were greatly improved (Nonaka & Takeuchi, 1995). Conversely by overlooking the need to formulate a clear business case in TELE-Co, its KM implementations were not as successful as CME-Co's (Coakes, 2004). This is even more evident in the improvements made in the ISS functions in adhering to regulatory requirements to manage ISS knowledge. KM impacted the two organisations primarily indirectly in exploiting intangible assets which were difficult to measure (Smith & McKeen, 2004). Unfortunately, the organisations isolated their KM initiatives in CS (Hansen et al., 1999) focusing on the operational side of KM as opposed to an integrated approach. CME-Co did collaborate in the generation of solutions with partners through an extranet but not internally with other functions. The ISS functions did not use a KM initiative but their management of knowledge was function specific, collaborating only vendors, auditors, stakeholders and regulatory bodies. IS Security functions have significantly impacted the organisations. Figure 7.6 presents a synthesised representation of the different types of potential IS Security KM Impacts.

The IS Security strategies were aligned to the corporate strategy ensuring that IS Security was mapped to every organisational technology and process within CME-Co and TELE-Co.

7.2.6 A Synthesised Perspective on Managing IS Security Knowledge

IS Security was used by the two organisations to participate in regulatory bodies to steer the markets. An inefficient IS Security function would result in corporate breaches and loss of earnings. The CS knowledge management initiatives were not aligned to the business strategies and as a result were dependent on the CS practitioners who are driving the use of KM tools and processes. KM was also specific to Customer Support. CS costs were reduced and time saved. CME-Co identified the advantage in pushing more and more knowledge towards partners. Customer loyalty was increased when the organisation became more open and willing to share knowledge. Therefore the two organisations have benefited from managing knowledge. CS utilised a KM initiative to positively impact the CS function and IS Security managed knowledge due to environmental requirements. However CME-Co through its CS function also identified market niches to target and ultimately increased profits. The CME-Co functions have been positively impacted by managing knowledge. To benefit from the lessons-learned from this analysis the CS the IS Security functions in the two organisations could exploit case-based reasoning tools and devise incentives for IS Security practitioners to become problem-solving gurus.

7.3 Aligning Information Systems Security to a KM Environment

This section addresses the third research question. The purpose of which is to determine how firms align IS Security to a KM environment. This section is an extension of the preceding sections which discussed the organisational infrastructure necessary to facilitate IS Security knowledge management (section 7.1). The IS Security knowledge, reservoirs and processes used to facilitate and control the CME-Co and TELE-Co KM environments were also described, compared and contrasted to illustrate how IS Security is aligned to the CS functions operating within the two case organisations investigated. Additionally the mechanisms used and the impacts of KM were discussed not only as tools to promote IS Security KM but to again illustrate the relationship between IS Security and the two KM environments (section 7.2). Therefore this section (7.3) extends sections 7.1 and 7.2 and explains how IS Security is aligned to a KM environment.

7.3.1 Interpreting IS Security Control through Governance

IS Security management and functions must understand the firms internal and external environments to build a suitable IS Security solution through effective ISS governance and quality control. This is achieved through the identification of IS Security responsibilities, practices, regulatory compliance, security policies, stakeholder relationships and IS Security activities to a KM. Ultimately, it is the responsibility of management to align IS security activities to a KM environment. IS Security must then be mapped to every business function, practitioner, process and technology (Patterson, 2005). This section describes the IS Security infrastructure used to protect a KM environment (sub-section 7.3.1.1), the environment under analysis (sub-section 7.3.1.2), IS Security controls necessary (sub-section 7.3.1.3) and IS Security auditing process (section 7.3.2). This section concludes with a synthesised perspective of the controls necessary to protect a KM environment.

It is the IS Security infrastructure which secures the organisation and assures the value and utility of its knowledge stores (O'Dell et al., 2004). The type of infrastructure used determines the level of access employees have to the knowledge that resides within a firm. Logical access rights were used to control access to CME-Co and TELE-Co knowledge stores. Best practice standards in the two organisations were crucial in establishing behavioural controls for decision-making. Corporate codes of ethics and ISS culture were introduced and delivered through security, education training and awareness (SETA) programmes. The two case organisations used M-Gates and Six Sigma (incorporating ISS gates and quality assurance steps) to ensure all employees utilised the same terminology in collaborating and managing projects across different business and support functions.

It is the role of senior ISS management to guarantee that its structure is supportive of the exploitation of KM initiatives, without necessarily impeding business processes. The two case organisations identified the competitive advantage that can be gained from incorporating security enhancements into their products, steering standard making bodies and providing a one-stop-shop for customer compliancy requirements. As a result roles and official groups were established in the two cases raising the profile and political power of the IS Security functions. The two case organisations have established formal IS Security functions with political, structural, and budgetary independence. The cases were proactive in ensuring their compliance with the required regulations to operate across different geographies but also in identifying customer demand for security enhanced products and services. The Corporate Security group established in CME-Co represented corporate stakeholders (customers, shareholders, and partners) by identifying their product, service requirements and aligning security to the strategy of the organisation. The new reporting structures for the two case organisations required ISS to report to the Finance and legal departments. External reviews from auditors and consultants forced a significant change in the importance of the two IS Security functions. TGS like the OISRM group analysed potential risks by improving IS Security processes to ensure a secure infrastructure for employees through proactive security strategies (policies, secure technologies and business assessment methodologies). TELE-Co also created a group responsible for developing global security procedures and policies which have disseminated to the various subsidiaries. Locally security is managed by Security Officers who are responsible for the security needs and audit reviews of individual sites. Securing a corporate network that has subsidiaries scattered around the world is a huge undertaking. In order to protect geographically dispersed subsidiaries the IS Security functions utilise Security Officers or Coordinators. These roles have the responsibility of rolling out the standards and controls selected by the corporate groups. They then collaborate using the different KM mechanisms used by TELE-Co and CME-Co. Senior management through, IS Security governance, are responsible for aligning the IS Security organisational infrastructure to a KM environment in order to support and protect it.

7.3.1.1 IS Security Governance

The relationship between governance and IS Security in CME-Co and TELE-Co exists in a number of different forms. The corporations are responsible to their creditors, stakeholders and for legal requirements (Dhillon, 2006). However ISS senior manager's corporate officers are responsible for IS Security through the application of formal (policies, procedures and audits), technical (compliance, access lists and audits) and informal (ethics and behaviours) controls. Corporate officers within the two case organisations must and have demonstrated responsible behaviour and met compliant

requirements (Kaen, 2003) through corporate governance. Corporate governance is concerned with who has legal control (Kaen, 2003; Borodzicz, 2005) which did create challenges for CME-Co and TELE-Co management. The ISS functions were impacted by the Sarbanes-and-Oxley (SOX) Act of 2002 which required better business and IT controls in legislation (Chou, 2005). It was through the ISS functions that tighter access controls for the organisations and therefore the KM environments were assigned. The allocation of senior responsibility through corporate governance has increased corporate security awareness (Kaarst-Brown & Kelly, 2005; CSI/FBI, 2006). The creation of the TGS and OISRM groups within the two case organisations dramatically increased awareness and made huge impact on the coordinated effort to comply with regulations across the two multinational organisations. However CME-Co additionally created a global ISS director with the sole responsibility of sourcing best practices and standards for the organisation giving ISS significant political power within the organisation. An ISS stakeholder group was also created to identify ISS niche market and target compliance as a potential source of income. An initiative which has not been addressed in literature, other than warnings regarding vendor bias (Stewart, 2005) and market fragmentation. CME-Co and TELE-Co corporate governance defines the control structure and control of tangible and intangible information assets and corporate knowledge which emphasise accountability and methods of auditing and control as discussed by Sundt, 2006.

Trompeter and Eloff (2001) argue that organisations should use confidentiality, integrity and availability (C.I.A) standards and security services to govern IS Security. However, while the two organisations regard these as implicit, both believed compliance and optimal balance as imperatives to ISS. Failure to comply with regulations would result in removal from the stock exchange and every organisation struggles to achieve optimal balance in assuring security without impeding productivity. Smith and Hasnas (1999) contend that the adoption of a code of ethics can have significant consequences (Reynolds, 2003). IS Security managers must therefore choose between competing ethical stances (Smith & Hasnas, 1999). However neither case organisation stressed the importance of the adoption of a code of ethics, as compliance, it was felt as enough. This contradicts the ISS literature as ethics is considered far more important (Whitman, 2004; Sundt, 2006).

Failures in governance have been due to a lack of awareness and conflicts of interest. As a result the case organisations stressed SETA and compliance as vital controls in any environment (CSI/FBI, 2006). There is a fundamental requirement for the governance of IS Security. Moulton and Coles (2003) refer to security governance in terms of: IS Security responsibility and practices, strategies and objectives for security, risk assessment and management, resource management for security, compliance with legislation, regulations, security policies and rules, investor relations and communication activities. CME-Co and TELE-Co have both made significant changes to ensure ISS governance which was relatively insignificant prior to 9/11 and SOX. Ultimately it is the responsibility of CME-Co and TELE-Co senior management to align security activities with the goals of the organisation (IT Governance Institute, 2001) and its KM environments. However, as CS and Engineering functions were prioritised other functions suffered from lazed security measures creating weak points in the corporate networks (Baskerville, 2004; Dhillon, 2006). Therefore IS Security was not mapped to every business function and process as advocated in literature (Patterson, 2005).

7.3.2 Interpreting the KM Environment in CME-Co and TELE-Co

CME-Co and TELE-Co operate in a business environment that is influenced by rapid technological advancement, high demand and short product lifecycles and therefore a high level of uncertainty. Evolving with the market place is therefore an imperative. The KM environments identified in the CME-Co and TELE-Co was the Customer Support functions. Technological and non-technological KM mechanisms were used extensively in the two case organisations (sections 5.1.6 and 6.1.6). There are risks and consequences through the utilisation of KM mechanisms that if not correctly controlled and reviewed, may in fact breach the security concerns of an organisation as well as privacy and regulatory controls. This section addresses these issues and provides guidelines in aligning IS Security controls to a KM environment through an analysis of the two case organisations investigated in this study. In identifying the correct controls to allocate to a KM environment it is necessary to identify the different KM resources used and then to identify the risks associated with the resources. Figure 7.7 (parts (a) and (b)) is used to diagrammatically illustrate the KM environments of the two case organisations investigated in this study. The illustration is based on the descriptions provided in Chapters 5 and 6. The KM resources used were numerous. However, they can be categorised into three: (1) individual and groups of experts, (2) paper-based document management systems and (3) KM technologies.

(1.) **Individual and Groups of Experts**

The first category was the users of the systems (individuals), the functions, and partners (customers and vendors). Individuals file reports, minutes, presentations, fill-in solution templates and standard operating procedures such as the SRD (security requirements document) and ISO17799. These were either stored electronically or by paper. Primarily they were uploaded to Primus and Compass, the central repositories used by the Customer Support functions. CME-Co and TELE-Co employees were allocated resources based on their role and responsibilities within the case organisations. Therefore, access to knowledge resources is domain specific. As in the case of two domains interacting, an Engineer can bypass a domain control to physically or electronically (by email) provide a CS Technician with a sensitive solution. However, Engineering repositories and tracking systems were partitioned from other functions. Role-based allocation of access rights is a requirement of compliancy regulations and it was the IS Security functions role to enforce these controls.

Figure 7.7(a) illustrates the access levels aligned to the different KM mechanisms in the TELE-Co and CME-Co KM environments. Access to the KM mechanisms, was administrated with four access levels to control its use. Level 1 was the most basic level. It was the Intranet entry point, providing company information, miscellaneous content, search functionality and hyperlinked documentation. Level 2 provided the user with content integration across projects and functions (standard function information), a more advanced search functionality, expert directories and users could personalise their views. Level 3 was categorised as a workplace integration level. It facilitated functions such as Customer Support in their operational activities, enabled collaboration, role-based (personalised) workflows and ERP (enterprise resource planning) integration (access to the corporate inventory systems). Level 4 facilitated marketplace integration, procurement support, and supply chain management. However, CME-Co provided access to its external partners. TELE-Co, for specific projects, provided partners with access to the Extranet in order to enable collaboration. Primarily, TELE-Co Engineers used VPNs to link to customer environments and solve product errors. Access to Primus

was provided externally to CME-Co key partners to enable them to directly contribute to the CBR tool. Resellers, service enabled partners and third party maintenance providers all had the ability to view (controlled) solutions through Power-Link (the CEM-Co Extranet). Partners and customers could author solutions which allowed Customer Support to capture potential bugs/ issues that the partners identified. Partner solutions were captured so that TELE-Co and other partners could share solutions. Capturing solutions from CME-Co partners was a valuable process. However, the solutions had to be properly reviewed and validated before they could be shared with other partners. CME-Co would be held responsible for any errors or potentially dangerous commands. Reviewing was a significant element of the process so that solution quality could be monitored. Providing partners with access to the central repository helped to open-up solution knowledge into a single, shared resource enabling CME-Co to allow partners to solve their own problems through a web-based self-help service.

The iView (interface) for Primus was optimised for partner or customer use. The system was used for searching, creating, using and managing solutions. Access was provided through a secure Extranet (Power-Link). Customers and partners, once registered to use the system, were automatically directed to iView instead of a generic Primus view. To provide the necessary control, partners cannot approve solutions. Only approved solutions could be viewed through Power-Link. All partners were associated with one of two groups aligned to the Primus application:

- Partner-Reader: users accessed the Primus iView to search for solutions and log notes/ comments against an existing solution. They could not create new solutions or modify existing solutions. They could only view 'status approved' solutions.
- Partner-Author: users, assigned to this group, had the rights of the Partner-Reader group with the additional rights of being able to create and modify solutions identified by CS and Engineering.

The users working in the two case organisations utilised the corporate Intranets to collaborate between communities of practice and the different functions across the geographically dispersed organisations. Leveraged content to improve products and services, from the two case organisations, integrated self-service offerings through Compass (provided by the TELE-Co University), Knowledge-link (provided by the CME-Co University), and access to online (public) help to reduce problem-solving time. The two case organisations used public forums and vendor repositories to pull external knowledge to solve problems. Encrypted virtual private networks were used to tunnel a secure connection between the two case organisations and external parties. However, TELE-Co utilised a human control mechanism in the form of site Export managers to verify and assure that any form of communication between TELE-Co and an external partner did not breach international or U.S laws regarding encryption.

(2.) **Paper-based Document Management Systems (DMS)**

IS Security procedures and standards, such as the ISO17799, were purchased and customised by the two case organisations. These standards listed the steps the IS Security functions should follow to comply with regulations and to protect the case environments. The procedures chosen were used to support the different SOX requirements for TELE-Co and CME-Co. Solution templates were used to ensure solution writers adhered to the quality control measures determined by the CS functions

within the two case organisations. Templates were used to ensure that solutions could be tagged for searches. The DMSs enforced by two case organisations specified the tagging of documents to determine their use and ownership. The DMS enabled users to convert the search functionality across to Compass and Primus. The documents stored were used to automatically and dynamically create solutions or bodies of knowledge. Documents describing similar problems and solutions were assigned to products or problems (accessing the different knowledge domains). CME-Co also used the tagging process to track solution usage through Primus. Call escalation procedures were used to allocate specific experts to particular problems. These procedures were also cost-saving measures as the higher the escalation - the higher the cost of the fix. The two cases also assigned author responsibility to solutions and procedures so that quality was ensured. CME-Co used a quality assurance team to assess solutions created internally by CME-Co employees and externally by CME-Co partners. The KCS team (composed of CS Engineers) was assigned as reviewers to ensure that the solutions were accurate and of a high enough quality to be stored in the CBR tool. Additionally they determined the access rights of the solution so that the right user was connected to the right knowledge.

(3.) **KM Technologies**

The KM technologies used in the two cases varied from repositories, databases, internal and external forums, common shares to tracking mechanisms. The mechanisms can, however, be categorised (Table 7.4) as collaborative mechanisms, public forums, problem-solving, monitoring, tracking mechanisms and KM repositories. There were several benefits to the utilisation of repositories (Compass) and case-based reasoning tools (Primus). New hires or employees with new job responsibilities could climb the learning curve more efficiently by learning from other employees. Automatic updates or alerts regarding internally published documents describing problems and solutions helped individuals reuse results and avoid reinventing the wheel. The KM mechanisms used by the individuals working within the IS Security and CS functions provided a number of advantages in enhancing problem-solving processes and innovation:

(1.) A central resource: for documentation, corporate project descriptions, templates and presentations.
(2.) Stored solutions: can be accessed through function portals.
(3.) Advanced search capabilities: templates were used to enhance the search capabilities of the different repositories through Compass.
(4.) Global distribution of documentation: reduced the level of duplication in procedures and solutions.
(5.) Global / regional distribution of problems and solutions: central resource for trouble-shooting documentation.
(6.) Ease of updates: individuals could easily update solutions and procedures, which were tracked through a quality review process to increase quality as ownership of documents and updates, were assigned.
(7.) Ease of Access: resources were restricted by domains.

In order to protect knowledge resources from the threats identified in the two case organisations. IS Security controls should be aligned to counter the threats. Figure 7.7 (b) illustrates and Table 7.4 outlines the controls aligned to the KM mechanisms identified in the two case organisations. The controls were allocated to prioritised systems and repositories as identified by ISS management. The prioritisation of systems, databases and repositories was determined by the financial loss incurred if a critical system was down or loss of time to market.

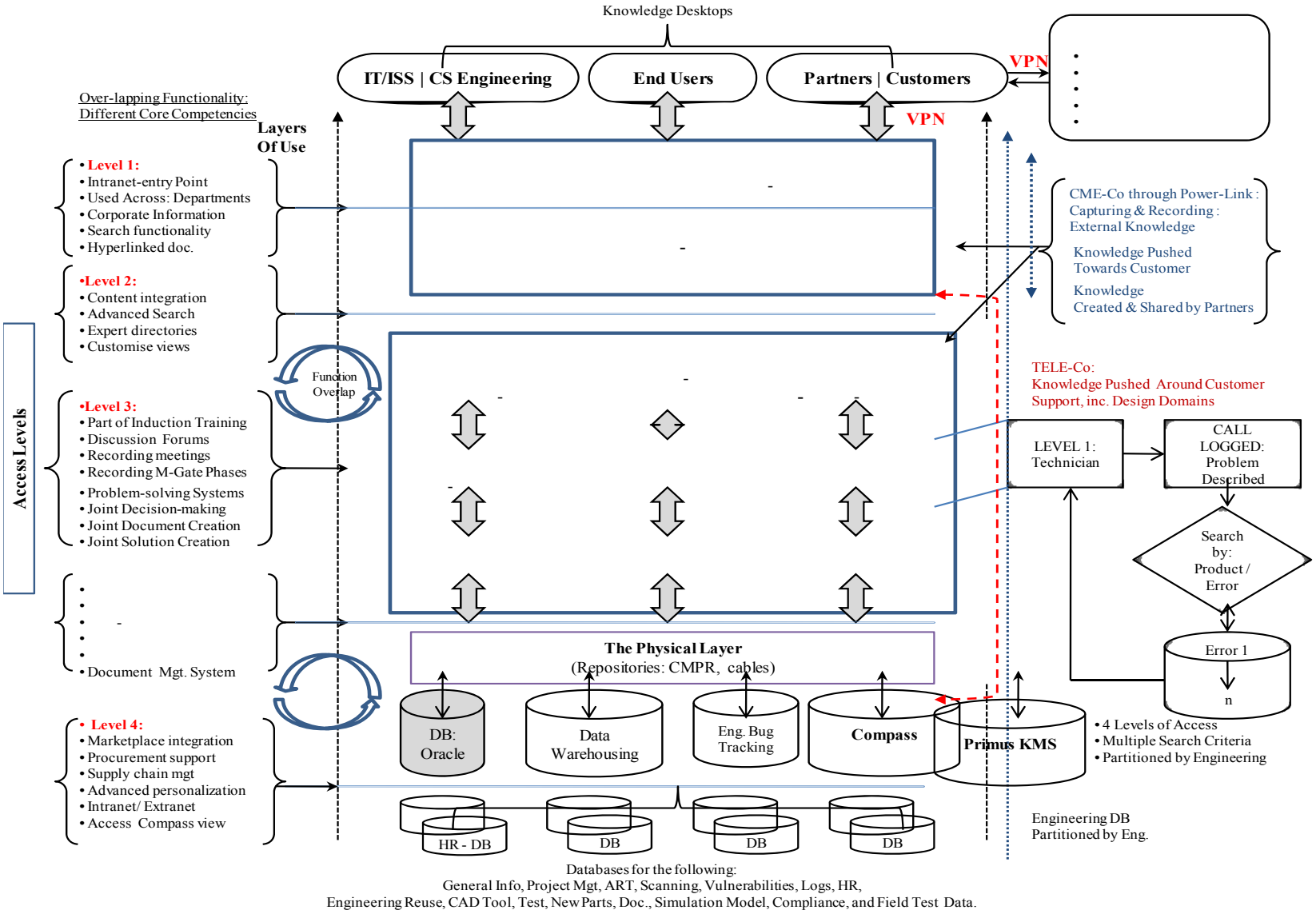

Figure 7.7(a): KM Environment

Time to market is very valuable to Engineering organisations. The two organisations have experienced instances when products were reverse-engineered and released by a competitor. Therefore, allocating the right controls to design databases and simulation models is vital. Primus and Compass as knowledge assets were prioritised and allocated significant security resources to assure the availability of the tools. IS Security controls were incorporated during the development and implementations of the different KM mechanisms utilised. Partitioning was used to control access of the different end-users to product solutions. This security measure was requested by Engineering to safeguard against inappropriate use of solutions. Engineering believed that some end-users lacked the technical knowledge necessary to understand the implications of specific commands and could potentially wipe-out a customer's data. This, however, resulted in cross functional conflict in CME-Co. Access controls permit or deny the use of an object by a subject. Access control systems provide the essential services of identification and authentication, authorisation, and accountability where identification and authentication determines who can logon to a system, authorisation determines what an authenticated user can do, and accountability identified what a user did. Strong authentication is often coupled with high investments in the security infrastructure (increases were made due to compliance). Virtual private networks (VPNs) utilised encryption when establishing connections over an existing shared infrastructure. Virus scanners functioned by constantly screening all inbound network traffic. Additionally product designs also needed to have allocated levels of access control.

7.3.2.1 IS Security Control Infrastructure

CME-Co and TELE-Co utilised a number of controls to protect their KM environments. The following types of controls or interventions were identified as countermeasures for the KM environments as illustrated in Figure 7.7 (b): KM hardware (sensitive knowledge access such as biometric access controls, regular audits of KM equipment, KM backups, physical security), KM software (automated procedures for KM access control, KM repository encryption), KMS development (KM system development methodologies such as the M-Gates were followed, validation and testing of KMS, quality assurance review), KM applications (systems access security, authentication, smart cards, encryption, backup and recovery), KM network controls (Internet, Extranet/Intranet access controls, virtual private networks, encryption, DMZ and firewalls) and KM human resources as identified by Jamieson (1991: 2004). Based on the requirements of the organisation and the type of KM initiative the appropriate controls should be selected by the IT/security groups and management as stated in literature (Jamieson & Handzic, 2004; Randeree, 2006). However, the CS functions in TELE-Co and CME-Co identified the necessary controls and ISS aligned them. ISS governance was not, as required by literature (IT Governance Institute, 2001), considered vital by the Engineering functions. Controls were therefore used as countermeasures to the perceived threat to the operations of the business, be it the management of knowledge, information or data. The process of ISS management involves identifying, assessing and evaluating the level of risk facing the two organisations (Borodzicz, 2006). It involves the identification of known threats (Williams *et al.,* 1995) and the process of risk engineering (Lievesly, 1995) or adapting to changing business environments.

ISS CONTROLS ALIGNED TO KM MECHANISMS		CME-Co	ISS Controls	TELE-Co
Non Technological				
Learning | Training KM Mechanisms:				
SETA:	Penalties for Breaking Security Procedures	√	Formal Control	√
Reviews:	6 month Assessment of Employees	√	Formal Control	√
Corp. University	Up-skill to meet Specific Needs	√	ISS Training	√
Collaborative Sessions:				
Teleconferences:	Used for Global Communication	√	NDA | External	√
Minutes of Meetings	Recorded & Stored	√	Stored: ACL	√
Meetings:	Face-to-Face	√	NDA | External	√
Brain Storming	Audit Reviews	√	NDA | External	√
Problem-solving	Collaborative Process	√	Stored: ACL	√
Documentation Quality Systems & Procedures:				
SRD:	Aligning Security Requirements to a Project	√	Doc. Controls	√
DMS:	Doc. Templates & Quality Procedures	√	Doc. Controls	√
Prj Mgt. Method	Phased approach to managing projects	√	Doc. Controls	√
Business Case	Project Resources & ID Roles Responsibilities	√	Doc. Controls	√
Individual & Groups of Expertise:				
Expert Status:	Expertise List	√	NDA | External	√
Global ISS Group	Global Security Function: Coordinate Teams	√	NDA | External	√
Global IP	Global Compliance Group	√	NDA | External	√
KM Team	Promote KM	√	NDA | External	√
KM Roles	KM Leadership	√	NDA | External	√
Symposia	Collaborate with Industry & Academia	√	NDA | External	√
Business Functions	Access depends on Roles & Responsibilities	√	Roles	√
KM Tools				
Collaborative Tools:				
Intranet:	Central Document Repository & Group Resource	√	Stored: ACL	√
CMS:	Stores Lessons-learned, Document Store	√	Stored: ACL	√
Groupware:	Collaborating & Sharing Solutions	√	Email Policies	√
Hyperlinks	Links to Internal & External Solutions	√	Email Policies	√
Common Shares	Groups, Regional Shares, Stores Procedures	√	Stored: ACL	√
Public Forums:				
Vendor Portals	Procedures, Guidelines and Best Practices	√	VPN	√
Extranet:	External NW	√	VPN	√
Forums	Public Collaboration	√	VPN	√
Problem-solving Tools:				
CBR	Case-based Reasoning Tools	√	ACL	
Simulation Models	System & Paper-based for Components	√	ACL	
CAD Tools:	CAD for Product Simulations	√	ACL	
MS Excel:	Risk Matrixes, to calculate the level of risk	√	Stored | ACL	
Monitoring & Tracking Tools:				
ART:	Automated Analysis, Reporting Tracking Tool	√	Monitoring SW	√
Scanning SW:	Monitors Rogues & Internal Employees	√	Monitoring SW	√
VPN:	Tunnelling to Protect Communication NWs	√	Encryption	√
Wireless Tech.	2-way Pagers for Call logging System	√	Notification	√
KM Repositories:				
Repositories	Legal liability regarding privacy etc	√	ACL	√
DB	Domain access	√	ACL	√
HR DB	Strict control	√	ACL	√

Table 7.4: IS Security Controls Aligned to KM Mechanisms

The ISS functions must understand their internal and external environments and the company's relationship (objective) with security before effective security solutions can be coined. The process involves implementing effective control measures (formal,

informal and technical) to maintain the optimum level of security (Marin, 1992; Dhillon, 2006). CME-Co and TELE-Co used a trial and error approach to targeting the optimal levels for their environments. In literature, this acceptable level is achieved through the introduction of a number of processes from risk, and feasibility analyses to the evaluation of IS security controls (Marin, 1992; Im & Baskerville, 2005). CME-Co and TELE-Co face enormous challenges in exposures to risks – be they security or otherwise.

Knowledge and expertise in the technologies necessary to alleviate IS Security risks were seen as valuable by the two case organisations (Dutta & McCrohan, 2002; Belsis et al., 2005; Stewart, 2005). Technology was used by the organisations to gather and share information while simultaneously protecting it. Therefore the ISS senior managers were familiar with some of the critical components of security technologies (Dutta & McCrohan, 2002). Technological changes, in both secure hardware and software, are as constant as the increase in the number of threats to corporate IS Security. Secure protocols, standards and encryption were used to protect business environments (Stallings, 2001; Dhillon, 2006) and IS Security technologies such as firewalls, scanning tools and intrusion detection systems are used to filter out possible threats (Jamieson, 1991). Theoretically the data derived from these tools should, if utilised correctly, provide an integrated view or knowledge pertaining to the IS Security landscape of the organisation (Belsis et al., 2005; Booz et al., 2005). CME-Co and TELE-Co, as illustrated in Figure 7.7, utilise a number of ISS technologies to build a complete view of their security landscapes.

As illustrated, a variety of controls were used to protect the data, information and knowledge stored by the two organisations. The most common counter measure is the firewall. Firewalls are regarded as the first line of defence of an IS Security strategy (Andress, 2004). Intrusion detection systems (IDS) monitor both inbound and outbound activities of the network and computer systems for signs of IS Security violations (Escamilla, 1998). Having detected such signs, the IDSs trigger alerts to categorise and report them. The report is downloaded by an analyst who evaluates and initiates an adequate response (Whitman & Mattord, 2005). However, information overload was reported by the two organisations. Access controls permit or deny the use of an object by a subject. Access control systems provide the essential services of identification and authentication (Andress, 2003; Cheswick, 2003; Dhillon, 2006). Cryptography was used to encrypt and decrypt data allowing employees and the organisations to store sensitive information or transmit it across insecure networks (Stallings, 2001; Sundt, 2006) to customers and partners. Virtual private networks (VPNs) utilised encryption when establishing connections over shared infrastructure to enable the two organisations to collaborate with their partners. These same technologies utilised by the two organisations have caused ISS challenges for the ISS functions. Advanced firewalls and virtual private networks (VPN) have resulted in (unintentionally) fragmented Security compartments (Baskerville, 2004; Dhillon, 2006) making them difficult to monitor and control (Baskerville, 2004; Stewart, 2005).

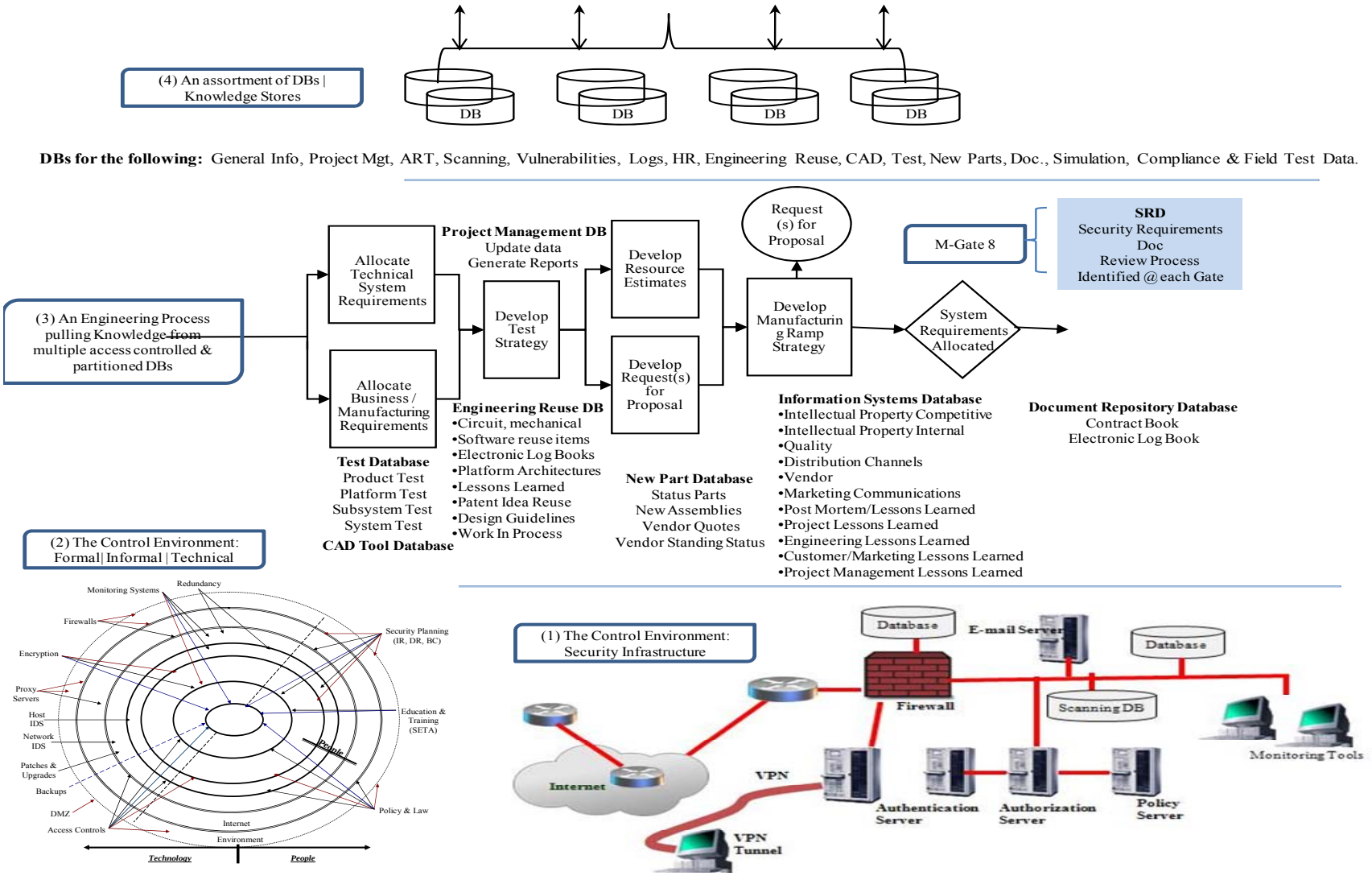

Figure 7.7(b): Aligning IS Security Controls to a KM Environment

Finally, the two case organisations were dependent on external reservoirs of knowledge for ISS tools, standards and best practices. Unfortunately the IS Security market is essentially vendor driven. IS Security capabilities (products) are widely available for any business to purchase (CSI/FBI, 2007). It is common practice (for vendors) to manipulate internal taxonomies of vulnerabilities to make vendor figures look more impressive, creating a false perception of value as warned by Stewart (2005). Vendors in the IS Security space have a vested interest in playing up the perception that organisations face rapidly increasing threats/risks, and ISS management should approach their claims with appropriate scepticism (CSI/FBI, 2007). However, vendors were used as a source of external knowledge and ultimately manipulated by the two organisations to varying degrees.

7.3.3. Interpreting IS Security Auditing Controls in the Case Studies

An elementary part of the IS Security function's responsibility is a careful examination of current regulations and common ethical expectations of national and international entities. Laws and regulations increasingly affect how IS Security is implemented (Sundt, 2006) in the two case organisations. Compliance has impacted KM processes as the documentation and application of access control rights to the different repositories, applications and databases used within the KM environments have increased. IS Security functions review the different KM mechanisms to determine the most effective security measures to allocate to the resources to prevent accidental or intentional damage, loss, modification, destruction or misuse of the mechanisms (Table 7.3). Unauthorised access, which is role-based, must be prevented and use histories (audit trails) were stored to ensure compliance. The KM mechanisms must be backed-up and network controls such as Extranets, access controls, VPNs, firewalls and dedicated connections were applied to the Primus CBR tools is available to customers. IS Security measures for protecting corporate knowledge, when shared internally were controlled through security policies, company ethics and enforced penalties. The IS Security functions therefore attempted to ensure that access is available to the correct users so that potential threats such as; loss of knowledge was eliminated.

The IS Security functions utilised a number of procedures, standards, checklists and best practices to ensure CME-Co and TELE-Co's compliance to different environmental regulations. TELE-Co enforced strict use of its DMS to control the quality of the solutions created. ISO17799 was identified by the two organisations as a vital IS Security guideline. While the two organisations purchased and customised externally produced standards, TELE-Co created in-house policies as behavioural controls in terms of protecting the organisations proprietary information (POPI). Engineers were reminded of penalties if they choose not to comply in TELE-Co. The case organisations have also hired compliance experts in order to try and understand the very complicated legal and compliance environment to adhere to regulations. However CME-Co extended the role of its compliance experts to identifying potential market requirements. Audit reviews were regarded as valuable sources of knowledge by the two organisations as externally sought evaluations of their IS Security functions. Review reports have been used as lessons-learned and checklists for the ongoing audit processes. M-Gates and Six Sigma were used by the two organisations as a common project management guidelines and (gate) vocabulary reference models to ensure organisational consistency across different projects. Usage varied within and across the organisations as CME-Co's IS Security function and TELE-Co's CS functions reported their use.

The corporate IS Security functions exploited IS Security repositories to automatically pull (multiple) firewall, scanning and IDS logs located throughout the corporate network in order to collate filtered knowledge into a prioritised list of issues for Security Officers and Coordinators. Subscriptions to technical repositories were used as a source of patch updates and procedures, and Q&A repositories. The IS Security functions exploited a number of security technologies to aid in monitoring and protecting their corporate boundaries. VPNs were used to encrypt lines of communication, SID for access-control and reporting, monitoring mechanisms to generate alert logs, firewalls for enforcing internal/external access rules and IDS to track internal and external network traffic. Additionally, TELE-Co utilised Excel to create checklists and to calculate risk levels. Scanning technologies, such as ART and Found-stone, were used to monitor the TELE-Co corporate network and track employees and rouges. While, scanners were used in CME-Co they were not reported to be as highly valued as they were in TELE-Co. However each technology generated streams of data which was pulled into monitoring databases in order to filter, query and generate a view of CME-Co and TELE-Co's security landscapes. Vendors are used to provide guidelines, product and technological specifications. The inter-relationships were formed to exploit financial opportunities. CME-Co established and utilised a Corporate Security group to analyse the security industry and identify stakeholder requirements. TELE-Co hosted IS Security and CS symposiums to identify the direction of regulatory and market requirements. The forums consisted of networks of IS Security practitioners collaborating and exchanging details regarding attacks, best practices and standards. Additionally the IS Security functions utilised external auditors as evaluators to adhere to regulatory requirements. The reports created were used as a form of measurement, a plan or checklist for future reviews and as a tool in post-mortem brainstorming sessions. It is also evident that both organisations are dependent on inter-relationships with external evaluators for IS Security. IS Security can be primarily differentiated by structural position in the two organisations by reporting to the Finance departments.

The auditing process forced the practitioners to undertake post-mortems at the end of a review which enhanced learning. Auditing has resulted in significant improvements in the two organisations. Processes are documented and knowledge regarding the organisations security status was constantly pulled from internal and external knowledge reservoirs. The efficiency of the IS Security processes were measured by determining the number of calls from customers and the number of improvements made as a result of an audit. CS processes were enhanced through employee rotation, brainstorming sessions and the recognition of practitioner contribution to the CBR tool. The number of solutions hits were measured and rated to create a competitive culture within CME-Co's CS function. Processes were also evaluated through the improvements made. Auditing techniques can be used to monitor a broad range of user and server security activities. It was recommended that practitioners routinely audit server configurations to detect areas where resources may be susceptible to unauthorised access and tampering. Therefore, auditing is an important ingredient of a secure KM mechanism. Audit records can notify operations staff that unauthorised access is being attempted. They can help IS Security functions to diagnose security breaches after they have occurred and give important information that will allow a practitioner to rectify security vulnerabilities.

7.3.3.1 IS Security Auditing

Environmental trends such as continued IT evolution and new business models coupled with strategies, such as knowledge management, have resulted in complex business environments on to which security must be mapped (Baskerville & Siponen, 2002). ISS governance is, as advocated by Ramos (2001), a key enabler in aligning the environment to the objectives of the organisations. Additionally, Jamieson & Handiz (2004) posited that IT governance should involve the governance of KM to ensure that it is aligned to the strategy of the organisation. Therefore, the ISS functions, as advised in literature, were consulted when considering security for the CME-Co and TELE-Co KM technologies, people and processes (Jamieson & Handiz, 2004). These personnel were responsible for identifying vulnerabilities and abuses associated with the systems (Whitman & Mattord, 2004) and implemented appropriate controls to alleviate identified threats. Management were also responsible for identifying and managing risks and the application of security controls to those risks. However, contrary to the literature KM governance committees were not created to identify knowledge assets within the two case organisations (Davenport & Prusak, 1998).

Auditors and security officers should also have been involved in the process. The ISS auditors did assess the adherence of the organisations to industrial standards such as COBiT (Control Objectives for Information and related Technologies) and ultimately compliance to regulations such as the Sarbanes and Oxley Act of 2002. Risks identified by the ISS functions were prioritised according to the threat posed to the CS and (primarily) the Engineering functions but not to KM (Jamieson & Handiz, 2004). Considerable risk is posed in establishing a KM project within the organisations. Additionally KM processes, technologies and knowledge workers should also be framed to identify the risks, if any, in generating, codifying transferring and sharing knowledge. One of the critical first steps in KM is to conduct a knowledge audit. Liebowitz (1999) contends that the audit is akin to the business needs assessment, therefore an aspiring "knowledge organisation" should inventory its knowledge assets. Neither of the two case organisations audited the KM environments within CME-Co nor do TELE-Co. Jamieson (2001) contend that knowledge auditing involves monitoring the usage of knowledge. However if the KM technologies utilised by the organisation do not have monitoring and auditing tools incorporated, Jamieson and Handzic (2004) advise that they should be added in order to protect and track the knowledge stored. The two case organisations did use auditing to evaluate the ISS functions within CME-Co and TELE-CO. Audits were effectively measures for the two ISS functions (Sundt, 2006). The process forced ISS to undertake post-mortems which unintentionally enhanced ISS learning. Auditing resulted in significant improvements. Processes were documented and knowledge regarding the ISS infrastructure was created and utilised. Auditing techniques were used to monitor a broad range of user and server security activities. These audits helped the IS Security functions to diagnose security breaches after they have occurred and give important information that will allow a practitioner to rectify security vulnerabilities.

7.3.4 A Synthesised Perspective on Aligning IS Security to a KM Environment

The relationships between IS Security and the KM environments in the two case organisations were very similar. The majority of the KM IS Security requirements were automatically aligned by the IS Security function. The goal of the IS Security functions was to ensure that the technical controls used are transparent to alleviate potential interference with internal processes. Security controls are incorporated during the

development of internal systems, particularly in partitioning systems. Partitioning was used to control the access of the different end-users to product solutions. This security measure is utilised by Engineering to safeguard against inappropriate access to product designs. KM does not affect the IS Security functions any differently than the steps needed to protect information systems. However it does experience difficulty controlling Engineering groups who ultimately "*circumvent security controls in the pursuit of innovation*". Engineers require and have full control over boxes (servers) and remove and add them to and from the corporate network as desired. IS Security officers are constantly battling with Engineering to adhere to the standards or guidelines and have implemented internal DMZs (demilitarised zones) as a separate control environment for developers. Full control of the network has caused serious network breaches and as result the unavailability, at times, of parts or the entire network. Failures, such as these, were considered by IS Security to be a barrier to the innovative process and a significant waste of resources in fixing the fault and loss of productivity due the unavailability of knowledge resources to other groups. However, Engineering has far more political support in the organisations and security is often sacrificed for the business case.

7.4 IS Security Leveraging KM

This section merges the findings identified in sections 7.1, 7.2 and 7.3 to describe and illustrate how IS Security can leverage the concept of KM. Each section addressed a component of the research framework (Figure 7.1) identified from the synthesised IS Security and KM literatures discussed in Chapter two (Figure 2.5) and set out in Chapter 3 (Figure 3.1). The framework was used as a lens to analyse the different factors and outcomes identified and to differentiate between them, based on their applications within CME-Co (Chapter five) and TELE-Co (Chapter six). The factors and outcomes acted as a basis for grounding the investigation of the approaches used to manage knowledge in two specialised support (IS Security and CS) functions. Sections 7.1, 7.2 and 7.3 addressed each of the research questions formulated in Chapter three. The organisational infrastructure necessary to support the management of ISS knowledge, how ISS knowledge should be managed and the alignment of IS Security to a KM environment are each described and compared to literature. This section describes and illustrates an IS Security KM model (Figure 7.8), derived from this investigation, as a guide for ISS practitioners in managing ISS knowledge.

7.4.1 The IS Security Model

To make effective decisions regarding IS Security, management must know about the various threats facing the organisation, its employees, data, information, knowledge and systems (Jones & Ashenden, 2005). ISS management and IT executives lack sufficient knowledge about their own vulnerabilities (Im & Baskerville, 2005) and the potential cost of failure (CIO, 2003) due to an inability to manage knowledge pertaining to IS Security (Belsis et al., 2005; Willison & Backhouse, 2006). IS Security function's and practitioner's knowledge of local threats, which form part of such risks, is often fragmented. The effectiveness of current approaches to managing IS Security knowledge has been questioned given the volume of security breaches. Management must not only minimise risks through the operationalisation of security activities but also effectively communicate vision, rules and guidelines to employees. Large volumes of data must be processed from a plethora of security technologies to provide information regarding the security landscape of the organisation (Stewart, 2005). As a result, management required the development of an integrated approach to the

management of IS Security knowledge. Combining security activities, experts and tools could resolve these problems. The application of a KM approach to the management of IS Security knowledge would enable a more holistic approach to the management of IS Security across an enterprise. Figure 7.8 is derived from the findings of sections 7.1, 7.2 and 7.3. The model illustrates the different components identified. Each variable is tagged with its corresponding sub-section to illustrate the flow of the ISS model. The remaining sub-sections outline the different components of the ISS model (Figure 7.8). The first three describe the types (sub-section 7.4.1.1), reservoirs (sub-section 7.4.1.2) and approaches (sub-section 7.4.1.3) used to manage knowledge, each of which is inter-dependent on the other. Sub-section 7.4.1.4 describes the KM mechanisms needed to promote KM in organisations. Sub-section 7.4.1.5 describes the expected levelled (individual, functional and organisational) impact of the approach. Sub-section 7.4.1.6 describes the infrastructure needed to support the management of ISS knowledge. Sub-section 7.4.1.7 outlines the controls necessary to protect a KM environment and finally sub-section 7.4.1.8 highlights the impact of the business environment the organisation is operating in.

7.4.1.1 Types of ISS Knowledge

The ability to problem-solve is vital and knowledge intensive. ISS functional general knowledge is primarily: operational, technical knowledge: tactical and contextual knowledge: strategic. Figure 7.8 (sub-section 7.4.1.1) presents a synthesised representation of the different types of IS Security knowledge an organisation should utilise. The practices of an ISS practitioner have changed due to technological advancements (Jashapara, 2004) and when individuals work in ISS functions to perform tasks, practitioners should create and apply ISS knowledge (Polanyi, 1966). The arrows represent the categorisation of IS Security knowledge as it is reused. Therefore, eventually contextually and technically specific knowledge will become IS Security general knowledge. As a result knowledge use and development is therefore regarded as a fundamental aspect of ISS activities (Gherardi, 2000; Hislop, 2005), making ISS knowledge inseparable from the actions of the ISS practitioner (Orlikowski, 2002). Equally, all knowledge work, whether using knowledge, sharing knowledge, developing knowledge or creating knowledge will involve an element of activity. ISS knowledge is pulled from corporate reservoirs of knowledge. The next section describes the different reservoirs from which ISS knowledge is pulled/ captured from.

7.4.1.2 Reservoirs of ISS Knowledge

The different levels of ISS expertise is a significant source of knowledge (Figure 7.8, sub-section 7.4.1.2). A considerable amount of knowledge resides in individual ISS practitioners (Argote & Ingram, 2000) and extensive knowledge resides within functions. Formal and informal knowledge development groups (Pan & Leidner, 2003) and coordinators can develop skill-sets and ensure solution standards. Procedures such as solution templates and management techniques are viewed as important sources of knowledge. Internal and external documentation can be sourced to comply with corporate requirements, such as lessons-learned and case solutions. Knowledge tools, repositories and email can be used to store knowledge. Inter-relationships with external evaluators for IS Security is an important source of measurement and best practices. Additionally, the utilisation of a stakeholder group to analyse the business environment can be a vital source of knowledge. Figure 7.8 provides a synthesised representation of the different reservoirs of IS Security knowledge an organisation should utilise. This knowledge, when processed, should be constantly changing and reused.

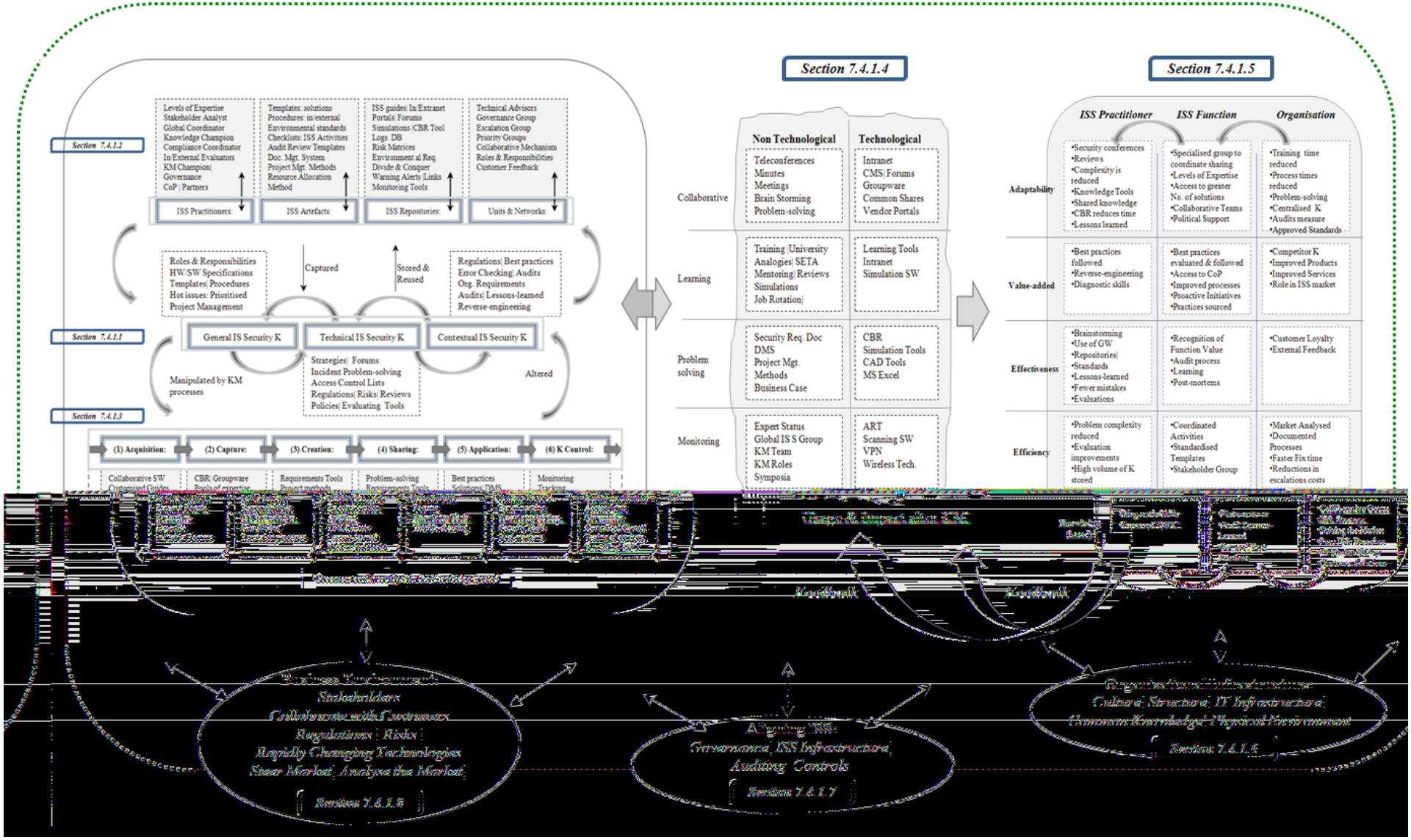

Figure 7.8: IS Security Leveraging the Concept of KM

7.4.1.3 ISS Knowledge Approaches

Figure 7.8 (sub-section 7.4.1.3) presents a synthesised representation of the different types of IS Security knowledge processes. ISS knowledge is *captured* from the different knowledge reservoirs (ISS technologies and pools of expertise) (Davenport & Prusak, 1998; Coakes, 2004). A significant amount of ISS knowledge is *acquired*. Collaborative software, regulatory guidelines, subscriptions, products and external evaluations are acquired by ISS functions to ensure that an organisation is compliant within their business environment and aware of any and all business opportunities (Holsapple & Singh, 2004; Baskerville, 2004). Problem-solving is the principal approach used to *create* ISS knowledge and applied through the reuse of the solutions created and stored. Collaborative software and trouble-shooting techniques can be used to *share* IS knowledge. The process of knowledge *application* relies on available ISS knowledge (Holsapple & Joshi, 2004). The auditing process can be manipulated to *use* reviews as benchmarking aids in applying lessons-learned to internal and external IS Security activities. Knowledge *control* is necessary to protect the ISS knowledge stored and used in an organisation. This is achieved through the allocation of controls such as tunnelling and quality control mechanisms (Jamieson & Handzic, 2004; Becerra-Fernandez et al., 2004; CSI, 2009). Controls are therefore used as ISS countermeasures to perceived threats to the operations of an organisation such as the management of knowledge. The processes identified should be used as an ongoing life-cycle of creating and using ISS knowledge. The next section describes the different mechanisms used to promote the management of ISS knowledge within an organisation.

7.4.1.4 ISS Knowledge Mechanisms

Use of KM mechanisms, in the context of this research, is measured in terms of the change which occurred as a result of managing knowledge either unintentionally or purposefully and the motivation to implement a KM initiative (O'Dell et al., 2004). The use of KM in either a general or specific context will affect its success (Gartner, 2000). If the level of use increases then KM will have a greater impact on the users (ISS practitioners and functions) and therefore the organisation (DeLone & McLean, 1992). The technological mechanisms, illustrated in Figure 7.8 (sub-section 7.4.1.4), are capable of combining explicit and tacit knowledge of ISS practitioners to varying degrees (Butler & Murphy, 2007). These technological and non technological mechanisms are categorised as collaborative, learning, problem-solving and monitoring tools. They can be used to acquire and manage knowledge and distribute it among the ISS functional groups as well as with any external collaborating partners (Alavi & Leidner, 2001) and therefore improving the effectiveness of decision-making (Peterson, 1996). The next section discusses the potential impact of managing ISS knowledge.

7.4.1.5 ISS Knowledge Impacts

ISS practitioner performance can be greatly impacted through the use of KM. It can facilitate individual learning and enhance exposure to the latest ISS knowledge through, for example, access to experts and lessons-learned from audit to audit. Employees can also be encouraged to learn from one another to adapt to inter-operability changes in their environments. Therefore, KM can facilitate employee learning and enhance their exposure to the latest knowledge in their fields of expertise. KM enables organisations and their functions to adapt quickly to changes in their environments, such as the IS Security landscape and technological advancements. These improvements can enhance

job satisfaction as skills were improved, as is the ISS practitioner's market value (Brown & Duguid, 1991). Knowledge mechanisms can be used to centralise IS Security knowledge and coordinate problem-solving. Therefore the IS Security practitioner role will become easier due to the utilisation of externally tested processes and practices. Specialised IS Security groups, if used, can coordinate and share knowledge across the organisation. KM can also facilitate improvements in organisational processes by improving the effectiveness, efficiency and innovativeness of the different processes to varying degrees. Specifically KM enables organisations and their functions to adapt quickly to changes in their environments, such as the IS Security landscape and technological advancements. The ISS functions can collaborate with vendors, auditors, stakeholders and regulatory bodies. Audits provide a measurement and facilitate learning through post-mortems forcing a proactive stance against IS Security challenges. Symposiums allow practitioners to collaborate with other organisations and academia. An organisation can use KM to improve their corporate products and services (Choi & Lee, 2002). Collaboration with partners can increase the number of ISS solutions and generate best practices. Solutions created and stored are reused which reduces the amount of time needed to solve problems. Audits force the recording of lessons-learned and therefore generate significant knowledge for future audits. The auditing process will have positive impacts for IS Security functions. It can force ISS practitioners to undertake post-mortems at the end of a review to enhance learning. To achieve these direct and indirect impacts IS Security strategies must be aligned to the corporate business strategy, thus ensuring that IS Security is mapped to every organisational technology and process within the organisation. Additionally, the flow of the arrows illustrate: the knock-on benefits to the organisation as individuals and functions are positively impacted by the approach. Finally, the cycle back illustrates that, as an organisation benefits from the approach more and more, resources will be allocated, thus improving its value.

7.4.1.6 ISS Organisational Infrastructure

In the preceding sub-sections the types, reservoirs and approaches used to manage ISS knowledge, through the ISS model were discussed. Organisational infrastructure is the foundation on which KM resides. It is composed of organisational: structure, culture, IT infrastructures, common knowledge and the physical environment (Standards Australia, 2001; Jamieson & Handzic, 2004). The structural component of the organisational infrastructure is vital in supporting the management of ISS knowledge. A separate ISS function will provide the specialised unit with political status, resources and budgets separate to IT (Dutta & McCrohan, 2002; Dhillon, 2006). Environmental drivers, specifically compliance, has both raised the status of the function and forced the documentation of processes and collection of knowledge regarding the security landscape of an organisation for external evaluations. Common organisational language and a culture of sharing need to be promoted in an organisation. Communities of practice should be created for internal and external collaboration. The co-ordination of KM requires the leadership of senior management if an organisation is to benefit from its utilisation (Hansen et al., 1999; Choi & Lee, 2002; Malhotra, 2000; Coakes, 2004). Additionally, the ISS function needs to participate in regulatory bodies to steer the ISS markets. The next section describes the controls necessary to protect a KM environment.

7.4.1.7 Aligning ISS Controls

The goal of the IS Security function is to ensure that the formal, technical and informal controls used are transparent to employees and to alleviate potential interference with internal processes. Controlling IS Security knowledge is a necessary aspect of the model (Figure 7.8, sub-section 7.4.1.7). Security technologies are used to control and protect IS Security knowledge resources. Systems (resources) were prioritised according to their value and controls aligned in order to protect IS Security knowledge pertaining to the organisation. Controls are allocated to IS Security documents to ensure quality, utility, consistency and ownership. Formal, informal and technical controls are used to control the behaviour of unauthorised users and knowledge pulled from the controls must be protected, restricted and monitored as its misuse could have serious consequences for the organisation. The next section describes the impact of the business environment.

7.4.1.8 ISS Business Environment

One of the fundamental problems regarding IS Security is for an organisation to choose the right kind of environment to function in. Strategic IS Security issues relate to where the firm chooses to operate and the scope of the organisation's relationship with other organisations. For example if an organisation chooses to work with a U.S. based firm. The organisation will have to ensure compliance with corporate governance as mandated by the Sarbanes-and-Oxley Act of 2002 (section 2.3.1). Moreover, any change to an existing business process will have implications for business partners.

Deficiencies in IS Security can cause direct negative consequences for business processes due to errors, delays and information leakage (Jamieson & Handzic, 2004). To make effective decisions regarding IS Security, management must know about the various threats facing an organisation, their employees, data, information, knowledge and systems when allocating resources, formulating security policies and performing risk assessments (Jones & Ashenden, 2005). The changes made to comply with regulatory requirements force ISS functions to acquire ISS knowledge externally from vendors, retrieve ISS knowledge from ISS technologies, create filtered reports highlighting internal and external threats, share this knowledge across the dispersed ISS functions and apply this knowledge for reviews and to ISS strategies. Therefore, in identifying the opportunity of utilising its external partnerships, such as vendors, to create additional knowledge and reduce support operational costs, is also vital (Borodzicz, 2005; Gal-or & Ghose, 2005; Booz et al., 2005; Dhillon, 2006).

7.4.2 Existing ISS Models

The IS research community has embraced many technologies as the "silver bullet solution" to corporate information needs (Webster & Watson, 2002). Previous IS Security research has been technical as criticised by leading IS researchers (Straub et al., 2008; Siponen & Willison, 2007; Dhillon, 2006). Similarly methods for the development of secure systems have been investigated (Baskerville, 1992; Siponen, 2005; Villarroel et al., 2005) while an integrated approach to managing IS Security has been ignored. Comparatively little work has taken a managerial point of view, covering broad organisational and social issues (Dhillon & Backhouse 2001; Straub et al., 2008). There are several frameworks which have been used to analyse Secure Information Systems (SIS) methods and approaches (Baskerville, 2004). Each study investigated

methods for secure IS, not the people, processes and technologies which embody IS Security functions (Siponen & Willison, 2007; Siponen et al., 2008).

Manunta (2000) contends that security is just a function of three components: an asset (A), a protector (P) and a threat (T). Security can therefore be expressed in any situation (Si) mathematically as: S = f (A, P, T) Si. However, this approach eliminates the complexity of understanding the concept of IS Security but the problem is compounded when applied in different environments (Baskerville, 1993; Wood, 1999; Baskerville & Siponen, 2002). Technical approaches to IS Security have limited effectiveness as security is primarily a people issue. IS Security requires the development of an integrated approach to the management of IS Security knowledge.

Another model used as a guide for the creation of knowledge is the 'spiral model' (Nonaka, 1991) of the different modes of knowledge creation or SECI. Nonaka's model has been hugely influential in demonstrating how knowledge is created and therefore how organisations should incorporate the management of tacit knowledge as a strategic objective. The leveraging of tacit knowledge is a difficult process and central to its achievement is the collaboration of the actors so that both tacit and explicit knowledge can be transferred to stimulate the creation of new knowledge. There are four modes of knowledge conversion involved in the process that leads to knowledge creation and the knowledge spiral which are socialization (is the process by which tacit knowledge from one individual is converted into the tacit knowledge of another), externalization (is the process of changing tacit knowledge into explicit), conversion (is a process of combining components of explicit knowledge) and internalization (is the process through which actors can personalise explicit knowledge and convert it into tacit knowledge) (Nonaka et al., 1996). Therefore, knowledge creation occurs when there is continuous interaction between tacit and explicit knowledge and produces a spiral effect; starting with one process and moving onto the new mode and so on. While the SECI model illustrates the importance of both knowledge types and the effect they have on each other and the way in which employees generate new knowledge from them. The model does not, however, address the goal of IS Security in minimising information systems operational risks. This involves several activities, such as planning, designing, implementing, monitoring, reviewing, and improving (BSI, 2002). These activities require specialised IS Security knowledge and one of the challenges faced by modern organisations is to acquire and manage expert knowledge in the area of IS Security (Belsis et al., 2005).

Existing IS Security models and procedures do not exhibit a high degree of flexibility, and as a result managers and IS Security practitioners make IS Security decisions in a knowledge vacuum. Risk can be managed or reduced when IS Security managers, practitioners and functions are aware of the full range of controls (formal/informal/technical), environmental threats, regulations, standards, technologies and practices available and implement the most effective solution. Threats should be met when organisations avoid reactive solutions and instead adopt proactive practices. To tackle threats or risks IS Security functions need to keep their skills and knowledge current. The effectiveness of current IS Security solutions and best practice standards have been seriously questioned (Baskerville, 2005). IS Security challenges increase the importance of managing IS Security knowledge in the context of protecting the organisation. Therefore, a customised model for managing ISS knowledge is required.

7.5 Summary

Combining IS Security knowledge, activities, experts and tools could resolve the different IS Security challenges encountered by organisations (Sundt, 2006; Randeree, 2006; Huo et al., 2008). This could be achieved through the utilisation of an effective KM approach. The application of the strategy to the management of IS Security knowledge would enable a more holistic approach to the management of IS Security across the enterprise. This chapter discusses how the different components of the organisational infrastructure can support the management of IS Security knowledge. It delves into the concept of managing IS Security knowledge to understand how organisations manage this knowledge. How firms align IS Security to a KM environment is discussed and a model is derived from this cross-case analysis. Ultimately, the researcher applied a KM approach to the management of IS Security knowledge to alleviate the challenges facing IS Security managers and functions. Approaches incorporating people and processes as well as technologies have never been contextually investigated. The administration and management of IS Security is a knowledge-intensive activity and to be effective must be managed.

CHAPTER EIGHT

CONCLUSION

8.0 Introduction

This Chapter takes the analysis of the findings and links these back to the research proposition and questions raised in response to the literature review, bringing a conclusion to the process, making a contribution to the gaps in the literature (Figure 1.1). This thesis aimed at exploring how Information Systems Security (ISS) could leverage the concept of Knowledge Management (KM) through qualitative research. This objective was divided into three questions that are recapitulated in section 8.1.

8.1 Findings

8.1.1 RQ.1: How can the organisational infrastructure support the management of IS Security knowledge?

A review of the literature revealed the importance of the organisational infrastructure in providing the foundation on which the functional units within reside and operate. The review revealed five main components (culture, structure, common knowledge, IT infrastructure and physical environment) that are traditionally depicted as interconnecting parts of an organisational infrastructure. Research has yet to explore their application in supporting the management of IS Security knowledge. The purpose of this research question was to use this theory as a lens to examine how the organisational infrastructure supported the management of IS Security knowledge in the two organisations participating in this study.

An analysis of the findings revealed the importance of the organisational infrastructure in supporting the needs of KM. The organisational infrastructure necessary to support the management of IS Security knowledge is evident in the two case organisations. However this is primarily due to the structural component of the organisational infrastructure. The two IS Security functions are formal departments in the organisations providing the IS Security functions with political status, resources and budgets separate to IT. Environmental drivers, specifically compliance, has both raised the status of the function and forced the documentation of processes and collection of knowledge regarding the security landscape of the organisations for external evaluations. Common organisational language and a culture of sharing are promoted in the cases. Additionally KM mechanisms are used throughout the two case organisations to facilitate knowledge sharing. However barriers to sharing appear to be more historic than environmental. The Engineering units in CME-Co and TELE-Co are reluctant to share knowledge due to the perceived risk of (design) knowledge becoming public or used incorrectly (high risk commands initiated in a customer environment). Knowledge sharing in the cases was function or team specific. The Customer Support function in CME-Co battles senior management, and particularly Engineering, to share internal knowledge. Changes in the business environment created a culture of security awareness for the two case organisations. The circumvention of (security) controls by Engineering created a culture of resentment from a security perspective as it weakens the control environment used to protect organisational assets. Therefore from a IS

Security and CS (front-line support) perspective a culture of entitlement and circumvention of rules created knowledge sharing issues for both functions despite the fact that security was aligned strategically to the goals of both organisations. Consequently, managing IS Security knowledge was vital in order for IS Security professionals to be proactive regarding security - particularly in sharing (SETA) threat and risk knowledge with the general employee population. Additionally external collaboration with CME-Co partners is proving effective in cutting costs in allowing customers and partners to "self-service" and even creates and shares their own solutions through the corporate Extranet. However TELE-Co uses a domain specific approach to KM. A community of practice (PKM) was created for collaboration across design domains not to collaborate across units or through inter-relationships. Therefore knowledge is pushed around the Engineering design domains and not to CS or the corporate customer base. Table 7.2 presents a synthesised representation of the organisational infrastructure components.

In the literature the importance of organisational infrastructure in supporting KM is high. Nevertheless, by overlooking the need to formulate a clear business case, many KM implementations fail (Coakes, 2004). Neither of the two case organisations support KM at a senior level beyond the creation of a corporate central repository. The co-ordination of KM requires the leadership of senior management if an organisation is to benefit from its utilisation. Even though many researchers highlight the importance of an overall KM strategy (Hansen et al., 1999; Choi & Lee, 2002; Malhotra, 2000; Coakes, 2004), it was not implemented in CME-Co or TELE-Co. KM has impacted CME-Co and TELE-Co directly and indirectly but only at functional levels. The literature has warned against companies isolating KM in functional departments such as CS (Hansen et al., 1999). The majority of organisations focus on the operational side of KM as opposed to an integrated approach. However the ISS functions did effectively (albeit indirectly) manage, due to the impact of compliance, their knowledge and benefited from structural, political and budgetary independence.

8.1.2 RQ.2: How do the two functional areas IS Security (ISS) and Customer Support (CS) manage knowledge?

The focus of research has been the technical side of security even though it has long been recognised that it is as important to understand the social elements of the area. Comparatively little work has taken a managerial point of view, covering broad organisational and social issues (Dhillon & Backhouse 2001; Straub et al., 2008). Scant work exists examining the management of security knowledge or secure knowledge management. Furthermore traditionally IS Security approaches have been grounded in positivism (Dhillon & Backhouse, 2001; Siponen & Willison, 2007). Previous studies have been neglectful in investigating IS Security as few if any studies utilised a qualitative approach, eliminating holistic, in depth rich descriptions of core issues within the field to facilitate the development of rigorous IS research and theory development. The literature suggests that the management of knowledge can directly impact the organisation at several levels: (ISS) individuals, the functions within, and the overall organisational performance. Impacts can come about directly from KM approaches or from the knowledge created, shared and applied through the approach. Therefore it is important to investigate how an organisation manages knowledge to determine the contribution of KM efforts.

The importance of IS Security knowledge can be attributed to the structures of the two organisations and their competitive business environments. IS Security is a futile

function if it is absent from the organisational structure. The ability to identify and react to rogues (hackers) is also viewed as strategic, emphasising TELE-Co's recognition of its expertise in rectifying security incidents. However proactive strategies were not identified by either organisation as an important skill indicating an inability to be proactive in tackling security challenges. CME-Co has identified compliance as a niche market and as a result formed a group to target customer regulatory requirements and generate additional income. The steps in applying standards for regulatory requirements are vital to the function. IS Security practitioners utilised regulatory and control knowledge to ensure compliance and follow external advice regarding audits. Different levels of expertise are viewed as a significant source of IS Security knowledge within the two organisations. CME-Co created ad hoc knowledge development groups and coordinators to develop lower level support skill-sets and ensure solution standards. Procedures such as solution templates and management techniques are viewed as important sources of knowledge. Knowledge tools, repositories and email were used to store knowledge. It is also evident that both organisations are dependent on inter-relationships with external evaluators for IS Security. A significant amount of knowledge was acquired externally. Collaborative software, regulatory guidelines, subscriptions, products and external evaluations were acquired by the functions to ensure that the organisations are compliant within their business environment and aware of any and all business opportunities such as market changes and competitor product advancements. Problem-solving was the principal approach used to create knowledge and applied through the reuse of the solutions created and stored. The IS Security functions purchased significantly more external knowledge than CS due to regulatory requirements However, this environmental driver enabled the IS Security functions to exploit the auditing process and use reviews as benchmarking aids in applying lessons-learned to internal and external IS Security activities.

CME-Co positioned its CS knowledge management initiative around a CRB tool. Due to the dedication of CS practitioners the role the tool was gradually increased as its value to CME-Co was continuously demonstrated. Additionally, Primus was used to provide CS solutions to and as a self-service support environment for CME-Co customers and partners. CS utilised quality mechanisms for the solutions created, allowed knowledge filtering, advanced search criteria's and pushed CS knowledge towards CME-Co customers. Therefore the IS Security functions were externally driven to comply with specific goals and measured due to regulatory requirements.

The IS Security functions have significantly impacted the organisations. The IS Security strategies were aligned to the corporate strategy ensuring that IS Security was mapped to every organisational technology and process within CME-Co and TELE-Co. IS Security was used by the two organisations to participate in regulatory bodies to steer the markets. An inefficient IS Security function would result in corporate breaches and loss of earnings. The CS knowledge management initiatives were not aligned to the business strategies and as a result were dependent on the CS practitioners who are driving the use of KM tools and processes. KM was also specific to Customer Support. However CS costs were reduced and time saved. However CME-Co identified the advantage in pushing more and more knowledge towards partners. Customer loyalty was increased when the organisation became more open and willing to share knowledge. Therefore the two organisations have benefited from managing knowledge. CS utilised a KM initiative to positively impact the CS function and IS Security managed knowledge due to environmental requirements

The effective management of IS Security is a knowledge-intensive activity that depends on the experience of security experts. Furthermore management must not only minimise risks through the operationalisation of security activities but also effectively communicate vision, rules and guidelines to employees. Large volumes of data must also be processed from a plethora of security technologies to provide information regarding the security landscape of the organisation. As a result management requires the development of an integrated approach to the management security knowledge. Combining the security activities, experts and mechanisms could resolve these problems. This was achieved through the utilisation of an effective KM approach, a solution which has been ignored by academia and industry. The application of the strategy to the management of security knowledge would enable a more holistic approach to the management of information security across the enterprise.

8.1.3 RQ.3: How can firms align Information Systems Security (ISS) to a Knowledge Management (KM) environment?

A review of the literature revealed that there is little if any accord regarding the relationship between IS Security and the management of knowledge other than the application of IS Security controls in the technological application of KM and vice versa. It is however agreed that both KM and IS Security involve people and processes as opposed to just technology. Therefore an organisation, through its IS Security function, must align IS Security to every facet of a KM environment to ensure that needed knowledge resources and processors are available in sufficient quantity and quality subject to the corporate IS Security measures and constraints. An organisation that intends to stay in business must have the necessary IS Security controls in place to prevent and certainly to decrease the frequency of loss. The purpose of the third research questions was to determine how firms align IS Security to a KM environment.

The corporate IS Security functions exploited IS Security repositories to automatically pull (multiple) firewall, scanning and IDS logs located throughout the corporate network in order to collate filtered knowledge into a prioritised list of issues for Security Officers and Coordinators. Subscriptions to technical repositories were used as a source of patch updates and procedures, and Q&A repositories. The IS Security functions exploited a number of security technologies to aid in monitoring and protecting their corporate boundaries. VPNs were used to encrypt lines of communication, SID for access-control and reporting, monitoring mechanisms to generate alert logs, firewalls for enforcing internal/external access rules and IDS to track internal and external network traffic. Each technology generated streams of data which was pulled into monitoring databases in order to filter, query and generate a view of an organisations security landscape.

Vendors are used to provide guidelines, product and technological specifications. The inter-relationships were formed to exploit financial opportunities. The forums consisted of networks of IS Security practitioners collaborating and exchanging details regarding attacks, best practices and standards. Additionally the IS Security functions utilised external auditors as evaluators to adhere to regulatory requirements. The reports created were used as a form of measurement, a plan or checklist for future reviews and as a tool in post-mortem brainstorming sessions. The auditing process forced the practitioners to undertake post-mortems at the end of a review which enhanced learning. Auditing has resulted in significant improvements in the two organisations. Processes are documented and knowledge regarding the organisations security status was constantly

pulled from internal and external knowledge reservoirs. Therefore IS Security is aligned to KM through IS governance, controls, and compliance.

ISS governance is, as advocated by Ramos (2001), a key enabler in aligning the environment to the objectives of the organisations. However, contrary to the literature KM governance committees were not created to identify knowledge assets within the two case organisations (Davenport & Prusak, 1998). Auditors and security officers should also have been involved in the process. Risks identified by the ISS functions were prioritised according to the threat posed to the CS and (primarily) the Engineering functions but not to KM (Jamieson & Handiz, 2004). Considerable risk is posed in establishing a KM project within the organisations. Additionally KM processes, technologies and knowledge workers should also be framed to identify the risks, if any, in generating, codifying, transferring and sharing knowledge. One of the critical first steps in KM is to conduct a knowledge audit. Liebowitz (1999) contends that the audit is akin to the business needs assessment, therefore an aspiring "knowledge organisation" should inventory its knowledge assets. Neither of the two case organisations audited the KM environments within CME-Co nor do TELE-Co. Jamieson (2001) contend that knowledge auditing involves monitoring the usage of knowledge. However if the KM technologies utilised by the organisation do not have monitoring and auditing tools incorporated, Jamieson and Handzic (2004) advise that they should be added in order to protect and track the knowledge stored. Auditing techniques were used to monitor a broad range of user and server security activities.

8.2 Conclusions, Contributions and Further Study

IS Security is vital for the protection of the organisation but also in assuring activities such as knowledge management. Therefore IS Security has become a strategic enabler for business and can itself provide competitive advantage through the creation of value added services and products and the protection of assets from known threats through the allocation of (formal, technical and informal) controls. Thus, organisations seek practical approaches to protect the business.

Unfortunately, the IS Security community is bogged down in small-scale technical queries as the social aspects of IS Security are ignored resulting in fragmented research across the IS field. While models and standards are scattered through the literature they focus on the secure development of information systems and standards. These standards are inflexible and ignore the fact that organisations are different. As a result managers make IS Security decisions in a knowledge vacuum and their subsequent actions to cope with threats are less effective. Research to date has failed to provide an integrated approach to the management of IS Security knowledge. KM has not, to the knowledge of the researcher, been used as a possible solution even though it is concerned with ensuring that knowledge is available in the right form to the right processors (IS Security: technologies, practitioners and processors) whenever required.

Thus, this study explored how IS Security could leverage the concept of KM through qualitative research. In order to accomplish this, the importance of organisational infrastructure in supporting the management of IS Security knowledge in each organisation participating in this study was determined as it provides the foundation on which functions operate and reside. In order to determine how to leverage KM it was necessary to investigate how the organisations manage knowledge. It was impossible to properly investigate this at organisational level – given the size, uncertain business environments and structural complexity. However, examining how one function

(Customer Support), using a KM approach, can help establish a baseline for implementing the KM approach in another function (IS Security). By comparing the KM approach used in a Customer Support function with the IS Security function operating within the same organisation, the researcher was able to determine how IS Security functions manage knowledge. Additionally, in leveraging the concept of KM for IS Security is was important to determine how IS Security functions support and manage knowledge to effectively align IS Security to KM environments. In the case organisations investigated this was achieved through governance, countermeasures (controls) and compliance.

The main contributions of this research are as follows:

First, this study answers calls from researchers and practitioners in the IS Security community and industry as it addresses the need for an integrated approach to managing IS Security knowledge. This study addresses the need for holism, rigour, and empirical fidelity in IS research by positing an integrative conceptual model that can be employed to help explain and understand the interplay between the IS Security and Customer Support functions (specialised units) at a local level and across the two case organisations. The IS Security research community is restrained by small-scale technical questions as the social aspects of IS Security are ignored resulting in fragmented research across the IS field. There has been a consensus in IS Security research that IS Security can be more effectively managed if the emphasis goes beyond the technical bastion used for protecting intangible resources (Baskerville, 1993; Straub & Welke, 1998; Dhillon & Backhouse, 2001; Dhillon & Torkzadeh, 2006). This study provides a theoretical perspective on managing IS Security and knowledge to addresses the weaknesses in the phenomenon.

The second contribution relates to the application of KM to an IS Security challenge. Gaps exist in both the KM and IS Security literatures where a relationship between both fields has rarely if ever been identified. Albeit security is put forward as a necessary consideration in the design and implementation of Knowledge Management Systems (KMS) like any other development project but not as a consideration or aid in the management of knowledge as in simply providing the right knowledge to the right finger tips (logical control). The IS Security literature advocates access control, security policies, the integrity of information and environmental threats yet KM has been ignored as a solution when in the case of this research it enabled the construction of an integrated model for managing IS Security knowledge.

The third major contribution is this study's utilisation of an interpretivist approach to IS Security to provide rich contextual findings. Traditionally approaches applied have been grounded in positivism (Dhillon & Backhouse, 2001) and technocratic in nature (Willson & Backhouse, 2006). Predictable threats seem apt for being investigated through positivist approaches, whereas unpredictable threats lend themselves to an interpretive approach (Spagnoletti & Resa, 2007) and require investigation in a social setting. Descriptive understanding is one of the main contributions of this research. This study presents systematically, using the research lens derived from an analysis of the literature reviews in Chapter two, descriptions of IS Security and CS knowledge, reservoirs, processes, mechanisms and the organisational infrastructure necessary to support KM. This is a critical form of knowledge; essential for theory building in the field of IS Security. Research has focussed on the analysis, design and the technical development of secure systems. The contribution of this thesis, beyond the previous

studies, is to bring together research in IS Security and KM and introduce an interpretive approach to the management of IS Security knowledge.

The fourth major contribution of this study is its practical implication for management as practitioner's knowledge of local threats is often fragmented (Willison & Backhouse, 2006) which can result in security breaches. As circumstances change, senior managers and IS Security functions must have the ability to take more or less risk based on judgement, understanding and knowledge. As IS Security breaks become a ubiquitous reality for all users of information, there is a pressing need for a theoretical framework against which practitioners may diagnose problems, plan action and implement solutions. IS Security models and standards today do not exhibit much flexibility, therefore managers make IS Security decisions in a vacuum. IS Security problems can be managed or reduced when managers are aware of the full range of controls (formal/informal/ technical) available and implement those which are most effective. Unfortunately, they often lack this knowledge and their subsequent actions to cope with systems risk are less effective. To complement and augment existing research, this study addresses the need for an IS Security model to manage IS Security knowledge.

Based on the findings of the two case organisations, this research has established a model for the management of IS Security knowledge. The model is organised by type of knowledge, reservoirs of IS Security knowledge, processes, mechanisms to promote IS Security KM, impacts and the organisational infrastructure supporting the management of IS Security (Figure 7.8). The fifth contribution relates to the study's findings. These act to confirm and extend existing theory and exploratory research and provide unique insights into the complex nature of the phenomenon of managing IS Security knowledge. This study provides a timely answer to calls in the IS field for in-depth empirical research of a qualitative nature on the management of IS Security. This research has also argued that to solve the problem of managing IS Security and ISS knowledge; practitioners and researchers need to understand the deep seated practical aspects of an organisation. This research has questioned the support provided by the organisational infrastructure in managing IS Security knowledge. In addition to being of academic interest, the findings from this research are intended to be useful for IS Security and Engineering practitioners engaged in the management of knowledge. This research provides some useful insight into the issues and concerns for the management of IS Security and ISS knowledge.

8.2.1 Further Research

The possible approach used by IS Security to leverage the concept of KM put forward in this research study will need to be tested in a number of organisations, and it is likely that more concepts will arise from such empirical work. However the concepts put forward in this research are sufficient to provide a robust foundation to develop an integrated model for the purposes of undertaking applied research of practical significance for organisations considering managing IS Security knowledge more efficiently. Ultimately, referring back to the arguments presented in Chapters one and two regarding the significance of IS Security research and desire of researchers to focus on the technical side of ISS as opposed to the social elements of the ISS field, there is an urgent need to understand the processes and behavioural components of IS Security to improve the management of ISS in organisations and reduce the number of ISS incidents. Future research should expand the number of case organisations used, but in different sectors. An analysis of the application of the model in an organisational setting would generate interesting findings particularly in determining the impact of the model.

Further research could also include a qualitative and quantitative analysis of organisations, operating in the Irish manufacturing sector, which need to leverage the management of tacit knowledge. A study could galvanise existing knowledge research areas such as training and learning models, KM, KMS and LMS, identify a critical path for future research, provide a substantial portfolio of rich case studies, create and validate a model for enhancing employee skill-sets through an effective (life-long) learning model and ultimately to manage tacit knowledge based on the exploitation of knowledge management and learning/knowledge management systems.

8.3 Discussion

This section reflects on the research design, case selection, and the limitations of this investigation. It then discusses the findings, implications for practice and research, and opportunities for further research. The thesis ends with a reflection on the PhD process.

8.3.1 The Research Design

The main elements of the research design were: interpretive; two case-studies; semi-structured interviews using a questionnaire to help guide interviewees. The data was analysed using manual transcription of the interviews, and coding by hand was used in qualitative data analysis. In retrospect, while much of the research process was successful, there were problems which might have been solved by adopting different approaches. The reminder of this section deals with each aspect of this investigation. Interpretive methods, unlike experimental methods, allow the researcher little control. Access to the case organisations and to interviewees was varied, with some case organisations being very open with several willing interviewees, and some interviewees easy to reach and arrange to interview, others were more difficult to schedule. Research themes had been identified during the analysis of the literature, but others occurred during the pilot case study (step 4 of the CSP). When carrying out the research some things did not go according to plan, and because there is little control and it was necessary to re-visit cases to delve further into the phenomenon. However, this did require far greater access to interviewees and more time. Unlike a longitudinal case-study, two case organisations provides only a snapshot of the situation in time, which means that the change process is not observed, and that reports of events from the past may be unreliable. Due to the fact that the utilisation of two case organisations, incorporating a pilot case, is less in-depth than a longitudinal case-study a less rich analysis of the organisations is achieved. Difficulties with access with some organisations providing many interviewees, and others only a few can also affect the richness of the case descriptions. In retrospect it may have been more advantageous to use a single longitudinal case-study design, in an organisation where there was extensive access, although there would have been other limitations. The utilisation of semi-structured interviews allowed the participants to bring up topics they believed to be important, which added to the richness of the data, but it also means that not all of the interviewees addressed the same issues. Interviewees may raise issues or make statements for ulterior motives, and say things that are biased. If a more structured interview approach had been used, more consistent results from the case organisations might have been achieved. However, a more structured interview approach could also have produced less rich results and proved weak in terms of reliability and validity of data.

The data that was gathered through semi-structured interviewees was analysed utilising a manual process. Automated software such as NVivo was not used as it was deemed unnecessary. While transcription was a slow process it proved valuable in allowing the researcher to fully appreciate the richness of the data and enable effective data reduction while working through the interviews compared to the utilisation of a transcribers. However there were still errors. These errors were often caught by the researcher. In some instances there was noise or interference making the words hard to hear. In this instance the researcher made use of the field notes taken during and immediately after the interviews. NVivo could have been used as an alternative to manual typing and analyses. The main benefit from using software is convenience of storage and running queries. Therefore the use of software instead of the manual process used offered little if any difference.

8.3.1.1 Case Selection Methodology

The study of organisations is complex, as their processes are made up of many activities (Stamper, 1973; Nutt, 1984; Baskerville, 2004). Traditionally organisations have been viewed as formal systems concerned with inter-organisational (between the organisations and its environment) and intra-organisational (internal departments) information. Since computer-based systems have been used to automate the activities of these formal systems this view has evolved. The emergent belief of a number of studies is to view the organisation as an evolving or emerging social form (Baskerville, 2004; Dhillon, 2006). Consequently, the organisation allows different groups to interact with each other and the environment (Walsham, 1993). Emergent organisations endure continuous change which is beyond simple environmental adaptiveness, allowing them to operate effectively in highly competitive markets by maintaining continual agility (Siponen & Iivari, 2006). Vulnerabilities and threats emerge as these organisations and their information systems are remade (Baskerville, 2004). As a result the context of IS Security is changing. Consequently, emergent IS Security must cope with rapid changes in the organisation, shifting information systems and changing vulnerabilities and threats through the development of an integrated and agile approach to managing IS Security. Agile IS Security management is required to anticipate threats and rapid responses. Traditional IS Security management principles and approaches will endure in organisations which are static and non-competitive, protecting traditional systems from traditional threats.

8.3.1.2 Limitations

The purpose of this section is to identify the limitations of this study. Limitations of the research strategy refer to the shortcomings at any stage of the research. These stages include: the conceptual framework and research questions; the development of a research approach, data collection techniques, data analysis and the reporting of the findings. While many of the potential limitations were discussed in Chapter three and tested in Chapter four, this section recapitulates the key weaknesses of the research strategy in addition to highlighting specific limitations that were encountered. The methodological approach for this research has been interpretive and one of the limitations of interpretive research is its reflexive nature. Researchers must therefore recognise that they are part of the social world they study. We then tend to rely on common-sense knowledge to make judgements about the social phenomena under investigation. While conducting this research many such judgements were made. Positivists consider this aspect of interpretive as a limitation. However the experiences and findings gained from this research gave the researcher little justification for

rejecting common-sense knowledge while conducting the research. Another limitation identified pertained to some of the literature read. IS Security is at an early stage of development, few studies have been carried out to date in the area, particularly of a qualitative nature (Siponen & Willison, 2007; Siponen et al., 2008). Therefore some of the relevant literature found is not in academic journals, but in industrial journals (CSI/FBI). The latter, it may be argued, are produced for a different audience and with a different focus. Such journals rely to a large extent on the support of vendors but to protect against mistaking promotion for research, the researcher focused primarily on (when referenced) journal articles written by independent industry analysts which have been referenced by the IS community.

This investigation adopted an interpretive stance, and the research design used a selection of two case organisations, interviewing a limited number of interviewees in each of the case organisations (Table 3.3). The approach and design leads to the following limitations: in generalisability, reliability, and validity. First, although statistical generalisability was not the intent, it is important to note that because the number of cases is so small compared to the population of engineering organisations, it is not possible to demonstrate that any findings are statistically representative of the whole population of engineering organisations. Second, due to the interpretive stance taken the reliability of any findings could be brought into question, the findings and conclusions are a result of an interpretation of the data by the researcher. The researcher maybe also be bias in analysing the data and ignore contradicting evidence regarding preconceived theories. Third, because the findings are based on interview data it was also possible to question the validity of the findings because interview bias is almost impossible to eliminate (Easterby-Smith et al., 1991). Interviewees may recount events from a personal perspective which is at odds with the views of other participants.

8.4 PhD Process

The PhD process commences with a PhD candidate who may or may not have prior research experience. The initial MPhil phase is seen in the United Kingdom as a programme of research preparation. At the end of the MPhil phase, PhD candidates must transfer from MPhil to PhD by producing a transfer report and defending it in a viva. The transfer report consists of a literature review, statement of research objective, questions and research methodology. Candidates are also required to investigate the identified research objective and questions in two case organisations. The MPhil is largely a minor thesis to be conducted for the PhD. The transfer viva is a validation of the research undertaken, and evidence of the PhD candidate's capability to plan and carry out a research programme.

As the PhD progresses the author changes. Writing style is perhaps the least important but most noticeable aspect that is changed. Familiarity with the subject is another obvious change as the author becomes immersed in the study, but confidence in conducting research and the acquisition of research skills are also developed. The whole process might be summarised as a process of learning how to theorise, gather relevant data, analyse that data, use the analysis to reach an informed decision about the hypotheses and theory, and then communicate that decision, in hopefully an interesting way. The PhD process should be viewed as a collaborative effort between the PhD candidate, supervisors, colleagues and the wider community of IS researchers who are present at conferences and other events, authors of previous works upon which the research builds, and the internal and external examiners. The end result is research that is informative and public.

BIBLIOGRAPHY

Adam, F. and Healy, M., (2000). A Practical Guide to Postgraduate Research in the Business Area, Blackhall Publishing, Dublin, Ireland.

Adams, D, Nelson, R. and Todd, P. (1992). Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology: a Replication, MIS Quarterly, 16 (2): July, 1992, pp. 227-247.

Adler, N. J. (1991). International Dimensions of Organizational Behavior, 2d Edition. Boston: PWS Kent.

Aken, J.E. (1978). On the Control of Complex Industrial Organisations. Leiden: Nijhoff.

Alavi, M. and Leidner, D.E. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues, MIS Quarterly, 25 (1): pp.107-136.

Anderson, R. (1999). How to Cheat at the Lottery (or, massively parallel requirements engineering). Proceedings of the Annual Computer Security Applications Conference (ACSAC99), Phoenix, AZ, pp. 14–27.

Anderson, J. (2003). Why We Need a New Definition of Information Security, Computers and Security, 22(4): pp.308-313.

Andress, A. (2004). Surviving Security: How to Integrate People, Process and Technology (Second Edition), Auerbach Publications.

Argote, L., and Ingram, P. (2000). Knowledge Transfer: a Basis for Competitive Advantage in Firms, Organizational Behavior and Human Decision Processes, 82 (1): pp.150-169.

Avison, D.E and Fitzgerald, G. (1995). Information Systems Development: Methodologies, Techniques and Tools, Second Edition, McGraw-Hill Companies.

Avital, M. (2004). Bolstering Knowledge Management Systems with Appreciative Inquiry, Case Western Reserve University.

Backhouse, J., Hsu, C.W. and Silva, L. (2006). Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard, MIS Quarterly, 30: pp.413-438.

Balta, R. and Gaadingue, T.G. (2006). Reflecting on 20 SEC Conferences, Computers and Security, 25: pp.247-256.

Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys, 25: pp375-414.

Baskerville, R. (2004). Agile Security for Information Warfare: A Call for Research, in Proceedings of the Twelfth European Conference on Information Systems (Leino T, Saarinen T, Klein S Edition), pp. 155-164, Turku School of Economics and Business Administration, Turku, Finland. (ISBN 951-564-192-6).

Baskerville, R. (1988). Designing Information Systems Security. John Wiley Information Systems Series, Chichester, UK.

Baskerville, R. (1992). The Developmental Duality of Information Systems Security. Journal of Management Systems, 4: pp.1-12.

Baskerville, R. (1994). Research Directions in Information Systems Security, International Journal of Information Management, 14: pp. 85-387.

Baskerville, R. (2008). Challenging the Challenge: Measure what makes you better and be better at what you Measure, European Journal of Information Systems, 17: pp. 1-3.

Baskerville, R. and Siponen, M. (2002). An Information Security Meta-policy for Emergent Organizations. Logistics Information Management, 15(5/6): pp. 337-346.

Baskerville, R., Dhillon, G., Pernul, Gn., and Soares, F. (2005). Panel: Information Systems Security Standards: The solution or the problem? In Proceedings of the Thirteenth European Conference on Information Systems (Bartmann D, Rajola F, Kallinikos J, Avison D, Winter R, Ein-Dor P, Becker Jr, Bodendorf, F and Weinhardt, C.), pp. 1780-1782, Regensburg, Germany. (ISBN 3-937195-09-2).

Becerra-Fernandez, I., Gonzalez, A., Sabherwal, R. (2004). Knowledge Management Challenges, Solutions, and Technologies, Pearson Prentice Hall, Upper Saddle River, NJ.

Behara, R., Huang, C.D, and Hu, Q. (2007). A System Dynamics Model of Information Security Investments. In Proceedings of the Fifteenth European Conference on Information Systems (Österle H, Schelp J, Winter R eds.), pp. 1572-1583, University of St. Gallen, St. Gallen.

Belsis, P., and Kokolakis, S., (2005). Information Systems Security from a Knowledge Management Perspective, Information Management and Computer Security, 13(3): pp. 189-202.

Benbasat, I., Goldstein, D.K. and Mead, M. (1987). The Case Research Strategy in Studies of Information Systems, MIS Quarterly, 11(3): pp.369-386.

Bharadwaj, A.S. (1996). Integrating Positivist and Interpretive Approaches to Information Systems Research: A Lakatosian Model. Second Americas Conference on Information Systems, Phoenix, Arizona, August 16-18.

Bisson, J. and Saint-Germain, R. (2004). The BS 7799 / ISO 17799 Standard: For a Better Approach to Information Security, http://www.callio.com/bs7799/id,179, Accessed: 14/05/2005.

Bjorck F. (1996). Security Scandinavian Style. Interpreting the Practice of Managing Information Systems in Organisations. Ph.D. Thesis. Stockholm University and Royal Institute of Technology.

Blackler, F. (1995). Knowledge, Knowledge Work and Organisations: An Overview and Interpretation, Organization Studies, 16(6): pp1021-1046.

Bohn, R. (1994). Measuring and Managing Technological Knowledge, Sloan Management Review, Fall, pp. 61-73.

Boland, R.J. and Tenkasi, R.V. (1995). Perspective Making and Perspective Taking in Communities of Knowing, Organization Science, 6(4):pp. 350-372.

Booz, Allen and Hamilton (2005). Convergence of Enterprise Security Organizations, The Alliance for Enterprise Security Risk Management.

Borchgrave, A., Cilluffo, F., Cardash, S. and Ledgerwood, M. (2001). Cyber Threats and Information Security Meeting the 21st Century Challenge. Washington, D.C.: The Center for Strategic and International Studies.

Borodzicz, E.P. (2005). Risk, Crisis and Security Management, John Wiley and Sons Publishers.

Botha, R.A. and Gaadingwe, T.G. (2006). Reflecting on 20 SEC Conferences, Computers and Security, 25: pp. 247-256.

Bourgeois, L.J. and Eisenhardt, K.M. (1988). Strategic Decision Processes in High Velocity Environments, Management Science, 34(7): pp. 816-835.

Brelade, S. and Harman, C. (2003). Practical Guide to Knowledge Management, Thorogood, London, http://site.ebrary.com/lib/intel/Doc?id=10088321, Accessed: 23/03/2006.

Brown, C.V. and Magill, S.L. (1994). Magill, Alignment of the IS functions with the enterprise: toward a model of antecedents, MIS Quarterly, 18(4): pp. 371–403.

Brown, A.D. (2000). Making Sense of Inquiry Sense making, Journal of Management Studies, 37(1): pp. 45-75.

Brown, J.S. and Duguid, P. (1991). Organisational Learning and Communities of Practice: Toward a Unified View of Working, Learning and Innovation. Organisation Science, 2(1): pp.40-57.

BSI. (2002), Information Security Management – Part 2: Specification for Information Security Management Systems, BS 7799-2:2002, British Standards Institute, London

Buchanan, S., and Gibb, F. (2008). The Information Audit: Methodology Selection. The International Journal of Information Management.

Buchel, B. and Raub, S. (2002). Building Knowledge Creating Value Networks, European Management Journal, 20 (6): pp.587-596.

Burrell, G., Morgan, G. (1979). Sociological Paradigms and Organisational Analysis, Heinemann, London.

Butler, T. (2000). Conference on Information Systems (AMCIS), Making Sense of Knowledge: A Constructivist Viewpoint. AMCIS, Long Beach, California, 2000, pp. 1462-1467.

Butler, T. (2000a). Transforming Information Systems Development through Computer-aided Systems Engineering (CASE): Lessons from Practice, Information Systems Journal, 10(3):pp.167-193.

Butler, T. and Fitzgerald, B. (2001). The Relationship Between User Participation and the Management of Change Surrounding the Development of Information Systems: A European Perspective, Journal of End User Computing (US), Jan-Mar, pp.12-25.

Butler, T. and Murphy, C. (2007). Implementing Knowledge Management Systems in Public Sector Organisations: A Case Study of Critical Success Factors, 15th European Conference on Information Systems St. Gallen, Switzerland, 12.

Cantoni, F., Bello, M., and Frigerio, C. (2001). Lowering the Barriers to Knowledge Transfer and Dissemination: The Italian Cooperative Banks Experience, in Proceedings of the European Conference on Information Systems, Bled, Slovenia, pp. 665-673.

Castano S, Fugini, M, Martell, G. and Samarati, P. (1995). Database Security. ACM press, New York.

Checkland, P. (1981). Systems Thinking, Systems Practice. J. Wiley and Sons, Chichester.

Cheswick, W., Bellovin, S., Rubin, A. (2003). Firewalls and Internet Security: Repelling the Willy Hacker (Second Edition), Addison Wesley.

Choi, B. and Lee, H. (2002). Knowledge Management Strategy and its Link to Knowledge Creation Process, Expert Systems with Applications, 23: pp.173-187.

Chou, S. (2005). Embracing Compliance, Wall Street and Technology, 23(5): pp 47-48.

Coakes, E. (2004). Knowledge Management – A Primer, Communications for the Association for Information Systems, 14: pp. 406-489.

Computer Security Institute. (2001). Computer Security Issues and Trends: 2001 CSI/FBI Computer Crime and Security Survey, http://www.gosci.com, Accessed: 20/06/01.

Computer Security Institute. (2005). Computer Security Issues and Trends: 2005 CSI/FBI Computer Crime and Security Survey, http://www.gosci.com, Accessed: 23/0605.

Computer Security Institute. (2006). Computer Security Issues and Trends: 2006 CSI/FBI Computer Crime and Security Survey, http://www.gosci.com, Accessed: 15/06/06.

Computer Security Institute. (2007). Computer Security Issues and Trends: 2007, CSI/FBI Computer Crime and Security Survey, http://www.gosci.com, Accessed: 17/03/2007.
Computer Security Institute. (2008). Computer Security Issues and Trends: 2008, CSI/FBI Computer Crime and Security Survey, http://www.gosci.com, Accessed: 23/06/08.
Computer Security Institute. (2009). Computer Security Issues and Trends: 2009, CSI/FBI Computer Crime and Security Survey, http://www.gosci.com, Accessed: 23/06/09.
Conway, J. (2004). Identity, Place, Knowledge: Social Movements Contesting Globalization. Halifax, NS: Fernwood Books.
Cresson Wood, C. (2001). Why Information Security is Now a Multi-disciplinary, Multi-departmental, and Multi-organisational in Nature, Computer Fraud and Security, 16.
Croasdell, D. T. (2001). Learning Organisations: its Role in Organisational Memory and Learning, Information Systems Management, Winter, pp.8-11.
Croasdell, D.C. (2001). IT's Role in Organizational Memory and Learning. Information Systems Management, 18 (1): pp. 8–11.
Davenport, T. H. and Prusak, L. (1998). Working Knowledge, Harvard Business School Press, Boston.
Davila, A. (2000). An Empirical Study on the Drivers of Management Control Systems' Design in New Product Development. Accounting, Organizations and Society 25: pp. 383–409.
Davis, G. (1992). An Individual and Group Strategy for Research in Information Systems, in Information Systems Research, Galliers, Robert (Editors).
De Long, D. and Fahey, L. (2000). Diagnosing Cultural Barriers to Knowledge Management, Academy of Management Executive, 14(4): pp.113-127.
Deal T. E. and Kennedy, A. A. (1982). Corporate Cultures: The Rites and Rituals of Corporate Life, Harmondsworth, Penguin Books
DeLone, W.H and McLean, E.R. (1992). Information Systems Success: The Quest for the Dependent Variable. Information Systems Research, 3(1): pp. 60-95.
DeLone, W.H and McLean, E.R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update, Journal of Management Information Systems, 19 (4): pp. 9-30
Denzin, N. and Lincoln, Y. (1998). Collecting and Interpreting Qualitative Materials. Thousand Oaks, CA, Sage.
DeSanctis, G. and Gallupe, B. (1987). A Foundation for the Study of Group Decision Support. Management Science, 33(5).
Desouza, K. and Evaristo, R. (2003). Global Knowledge Management Strategies, European Management Journal, 21(1): pp. 62-67.
Dhillon, G. (1997). Managing Information Systems Security. MacMillan Press Ltd., London, UK
Dhillon, G. (2001). Information Security Management: Global Challenges in the New Millennium. Hershey: Idea Group Publications.
Dhillon, G. (2005). Gaining Benefits from IS/IT Implementation: Interpretations from Case Studies, International Journal of Information Management, 25(6).
Dhillon, G. (2006). Principles of Information Systems Security: Texts and Cases, John Wiley and Sons Publishers.
Dhillon, G. and Backhouse, J. (2001). Current Directions in IS Security Research: Toward Socio-Organizational Perspectives. Information Systems Journal, 11: pp.129-156.

Dhillon, G., and Hosein, I. (2001). Formal Methods and Secure Systems Development. Proceedings of the Information Resources Management Association conference, Toronto, Canada.

Dieng, R. Corby, O. Giboin, A. and Ribiere, M. (1998). Methods and Tools for Corporate Knowledge Management, Institut National De Recherche en Informatique et en Automatique, Rapport de recherché, September, Theme 3, No 3485.

Dojkovski, S., Lichtenstein, S. and Warren, M.J. (2007). Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. In Proceedings of the Fifteenth European Conference on Information Systems (Österle H, Schelp J, Winter R eds.), pp.1560-1571, University of St. Gallen, St. Gallen.

Douglas, M. (1970). Natural Symbols, Explorations in Cosmology. London: Routledge.

Doyle, S. (1997). Securing Electronic Documents, KPMG Global Knowledge Management Repository.

Drake, P., Shanks, G., and Broadbent, M. (1998). Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism, Information Systems Journal, (8): pp.273-289.

Drucker, P. (1993). Post-Capitalist Society, New York, HarperCollins.

Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cybereconomy, California Management Review, 45(1).

Earl, M., and Hopwood (1980). From Management Information to Information Management, The Information Systems Environment (Lucas H., Land F., Lincoln T. And Supper K., Edition.), Amsterdam: North Holland.

Easterby-Smith, M., Thorpe, R and Lowe, A., (1991). Management Research-An Introduction, London: Sage Publications.

Eisenhardt, K.M. (1989). Building Theories from Case Study Research. Academy of Management Review, 14(4): pp. 532-550.

Eloff M.M. and Solms S.H. (2000a). Information Security Management: A Hierarchical Framework for Various Approaches. Computers and Security 19: pp.243-256.

Eppler, M., (2004). Making Knowledge Visible through Knowledge Maps: Concepts, Elements, Cases, in Holsapple, C.W. (Edition.), Handbook on Knowledge Management 1: Knowledge Matters, Springer-Verlag, Berlin, pp. 189-207.

Erlandson, D.A., Harris, E.L., Skipper, B.L. and Allen, S.D. (1993). Doing Naturalistic Inquiry: A Guide to Methods. Sage Publications Ltd., London.

Escamilla, T. (1998). Intrusion Detection: Network Security Beyond the Firewall. John Wily and Sons. First Edition.

Eschelbeck, G. (2005). The Laws of Vulnerabilities: Which Security Vulnerabilities Really Matter? Information Security Technical Report, 10, pp. 213-219, Elsevier Ltd.

Ettinger, E. (1993). Information Security: an Integrated Approach. Chapman and Hall, Ltd.

Feltham, G. and Mbagwu, C. (2006). Misleading Disclosure of Pro Forma Earnings: An Empirical Examination, in Journal of Business Ethics, 69(4): pp. 355-372.

Fiol, C.M., and Lyles, M.A. (1985). Organizational Learning. Academy of Management Review, 10: pp.803-813.

Fitzgerald, G. (1991). Validating New Information Systems Techniques: A Retrospective Analysis, in Information Systems Research: Contemporary Approaches and Emergent Traditions, Nissen, H. and Hirschheim, R. (Editors).

Fontana, A., and Frey, J.H. (1994). Interviewing: The Art of Science. In N.K. Denzin, and Y.S. Lincoln, (Edition), Handbook of Qualitative Research. Sage Publications

Gable, G.G. (1994). Integrating Case Study and Survey Research Methods: An Example in Information Systems, European Journal of Information Systems 3(2). pp.112-126.

Galegher, J., Kraut, R.E., (1990). Technology For Intellectual Teamwork: Perspectives on Research and Design, in Galegher, J., Kraut, R.E., Egido, C., (Editors), Intellectual Teamwork, Lawrence Erlbaum Associates Publishers, New Jersey, pp. 1-20.

Galliers, R.D. (1991). Choosing Appropriate Information Systems Research Approaches: a Revised Taxonomy, Information System Research: Contemporary Approaches and Emergent Traditions, Elseiver Science Publishers, North Holland, pp.327-345.

Galliers, R.D. (1992). Choosing Information Research Approaches in Information Systems Research. In R.D. Galliers (Editors) Choosing Information Research Approaches In Information Systems Research: Issues Methods and Practical Guidelines, Blackwell, London.

Galliers, R.D. (1993). Research Issues in Information Systems, Journal of Information Technology, 8: pp. 92-98.

Galliers, R.D. and Baker, S.H. (1994). Strategic Information Management: Challenges and Strategies in Managing Information Systems, Oxford: Butterworth-Heinemann, 390 pp.

Galliers, R.D. and Newell, S. (2001). Back to the Future: From Knowledge Management to Data Management. In Global Co-Operation in the New Millennium, The 9th European Conference on Information Systems, Bled, Slovenia, June 27-29, pp. 609-615.

Galliers, R.D. and Newell, S. (2003). Strategy as Data Plus Sense-making, Images of Strategy, Edited by S. Cummings and D.Wilson, Blackwell Publishing.

Galliers, R.D., and Land, F.F. (1987). Choosing Appropriate Information Systems Methodologies, Communications of the ACM 30(11): pp. 900-902.

Gal-or, E., and Ghose, A. (2005). The Economic Incentives for Sharing Security Information, Information Systems Research, 16(2): pp.186-208.

Gaunt, N. (2000). Practical Approaches to Creating a Security Culture. International Journal of Medical Informatics, 60(2): pp.151-157.

Gerber, M. and Von Solms, R. (2005). Management of Risk in the Information Age, Computer and Security, 24(1): pp.16-30.

Gerber, M., Von Solms, R., Overbeek, P. (2001). Formalizing Information Security Requirements, Information Management and Computer Security 9(1): pp. 32-37, MCB University Press.

Gersick, C.J.G. (1988). Time and Transition in Work Teams: Toward a New Model of Group Development, Academy of Management Journal, 31 (1): pp.9-41.

Ghauri, P. and Gronhaung, K. (2002). Research Methods in Business Studies: A Practical Guide (2nd Edition), Harlow, Financial Times Prentice Hall.

Gherardi, S. (2000). Practice-based Theorizing on Learning and Knowing in Organizations, Organization, 7(2): pp.211-223.

Gibson, Q. (1960). The Logic of Social Inquiry, London, Routledge.

Gill, J. and Johnson, P. (1997). Research Methods for Managers, 2nd Edition, Paul Chapman, London.

Goldkuhl, G. (1996). Generic Business Frameworks and Action Modelling, In Proceedings of Conference Communication Modelling - Language/Action Perspective, Springer Verlag.

Gordon, G., and DiTomaso, N. (1992). Predicting Corporate Performance from the Strength of Organizational Culture, Journal of Management Studies.

Gordon, L., Loeb, M., Lucyshyn, W. and Richardson, R. (2006). CSI/FBI Computer Crime and Security Survey. Computer Security Institute.

Grant, R.M. (1996). Towards a Knowledge-Based Theory of the Firm, Strategic Management Journal, 17(Winter Special Issue), pp. 109-122.

Greenstein M. and Vasarhelyi, M. (2002). Electronic commerce, Risk Management and Control, Second Edition, McGraw-Hill.

Greenstein, M. and Feinman, T.M., (2000). Electronic Commerce: Security, Risk Management and Control, McGraw-Hill.

Guba, E.G. and Lincoln, Y.S. (1994). Competing Paradigms in Qualitative Research. In N. K. Denzin and Y. S. Lincoln (Edition), Handbook of Qualitative Research, Sage Publications Inc., CA, pp.105-117.

Guo, H. (2008). Knowledge for Managing information System Security: Review and Future Research Directions, International Conference on Information Resources Management (CONF-IRM), Proceedings, Association for Information Systems.

Hackett (2006). Sarbanes Oxley and IT Compliance, Hackett Group.

Hall, E.T. (1959). The Silent Language, 2nd Edition, New York: Anchor Books.

Hanley, S and Malafsky, G. (2004). A Guide for Measuring the Value of KM Investments, in Holsapple, Handbook on Knowledge Management, 2 Knowledge Directions, 2nd Edition, pp. 368-410.

Hansen, M.T., Nohria, N. and Tierney, T. (1999). What's Your Strategy for Managing Knowledge? Harvard Business Review, 77(2): pp.215-233.

Haworth, D.A and Pietron, L.R. (2006). Sarbanes-Oxley: Achieving Compliance by Starting with ISO17799, Information Systems Management.

Hayek, F.A. (1945). The Use of Knowledge in Society, American Economic Review, 35.

Hendriks, P. (1999). Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing. Knowledge and Process Management, 6(2): pp. 91-100

Hinde, S. (2002). Security Surveys Spring Crop. Computers and Security, 21(4): pp. 310–21.

Hinde, S. (2003). The Law, Cybercrime, Risk Assessment and Cyber Protection, Computers and Security, 22(2): pp. 7-17.

Hirschheim, R. (1985). Information Systems Epistemology: an Historical Perspective. Proceedings of the IFIP WG 8.2. Working Conference on Research methods in information systems. Elsevier Science Publisher, Amsterdam.

Hirschheim, R. (1992). Information Systems Epistoemology: An Historical Perspective, in Galliers, R., (Editor), Information Systems Research Issues, Methods, and Practical Guidelines, Blackwell Scientific Publications, pp. 28-60.

Hislop, D. (2003). The Complex Relationship Between Communities of Practice and the Implementation of Technological Innovation, International Journal of Innovation Management, 7(2): pp.163-188.

Hislop, D. (2005). Knowledge Management in Organizations: A Critical Introduction. 1st Edition. Oxford University Press.

Hislop, D., Newell, S., Scarbrough, H. and Swan, J. (2000). Networks, Knowledge and Power: Decision manking, Politics and the Process of Innovation, Technology Analysis and Strategic Management, 12(3): pp. 399-411.

Holsapple, C.W. and Joshi, K.D. (2000). An Investigation of Factors that Influence the Management of Knowledge in Organizations. Journal of Strategy Information Systems, 9(2): pp. 235-261.

Holsapple, C.W. and Joshi, K.D. (2004). An Ontological Representation of Learning Objects and Learning Designs as Codified Knowledge, Communications of the ACM, 45(2).

Holsapple, C.W. and Singh, M. (2004). Achieving Knowledge Management Outcomes, (Edition), Handbook on Knowledge Management 1: Knowledge Matters, Springer-Verlag, Berlin, pp 477-507.

Hong, K., Chi, L.R and Tang, J (2003). An Integrated System Theory of Information Security Management, Information Management and Computer Security, 11: pp. 243-248, MCB University Press [ISSN 0968-5227].

Hu, Q., Dinev, T., Hart, P., Cooke, D. (2008). Top Management Championship and Individual Behaviour Towards Information Security: An Integrative Model, in the European Conference on Information Systems.

Huang, M., Chen, M., and Show-Chin, L. (2007). Integrating Data Mining with Case-based Reasoning for Chronic Diseases Prognosis and Diagnosis, Expert Systems with Applications, 32: pp.856–867.

Huber, G. (1991). Organisational Learning: The Contributing Processes and the Literatures, Organisational Science, 2(1): pp. 88-115

Iivari J and Kerola P (1983). A Sociocybernetic Framework for the Feature Analysis of Information Systems Design Methodologies. In: Olle TW, Sol HG and Tully CJ (Edition). Information Systems Design Methodologies: A Feature Analysis, North-Holland, Amsterdam, pp. 87-139.

Im, G.P and Baskerville, R (2005). A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error, The Database for Advances in Information Systems, 36(4): pp. 68-79.

ISO/IEC TR 13335-4, (1997). Information Technology ± Security Techniques ± Guidelines for the Management of IT Security ± Part 4: Selection of Safeguards (Working Draft), ISO, Australia.

IT Governance Institute. (2001). Information Security Governance: Guidance for Boards of Directors and Executive Management, Rolling Meadows, IL: Information Audit and Control Foundation.

ITSEC. (1991). Commission of the European Communities, Information Technology Security Evaluation Criteria, Provisional Harmonised Criteria: Version 1.2. Office for Official Publications of the European Communities, Luxembourg, June.

Ives, W., Torrey, B., and Gordon, C. (1998). Anderson Consulting, Knowledge Management: An emerging discipline with a long History, Journal of Knowledge Management, 1(4).

Jackson, J. (1995). Preserving Indian Culture: Shaman Schools and Ethno-Education in the Vaupes, Colombia. Cultural Anthropology.

Jackson, S. and Philip G. (2010). An Emergence Perspective on the Management of Techno-change, International Journal of Information Management.

Jamieson, R. (1991). Auditing Expert Systems, Research Monograph No 3, Carol Stream, Illinois: EDP Auditors Foundation.

Jamieson, R. and Handiz, M. (2004). A Framework for Security, Control and Assurance of Knowledge Management Systems, in Holsapple, C.W. (Edition), Handbook on Knowledge Management 1: Knowledge Matters, Springer-Verlag, Berlin, pp. 477-507.

Jashapara, A. (2004). Knowledge Management, An Integrated Approach, Pearson Education Limited.

Jenkins, M. (1985). Research methodologies and MIS research, in Munford et al. (Eds). Research Methods in Information Systems, North Holland.

Jensen, M.C. and Meckling, W.H. (1996). Specific and General Knowledge, and Organizational Structure, in Myers, P.S. (Edition). Knowledge Management and Organizational Design. Butterworth-Heinemann, Newton, MA, pp. 17-38.

Jermier, J.M., Slocum, J.W., Fry, L.W., and Gaines, J. (1991). Organizational Subcultures in a Soft Bureaucracy: Resistance Behind the Myth and Facade of an Official Culture. Organization Science, 2(2): pp.170-191.

Johansson, E. (2005). Assessment of Enterprise Information Systems Security – How to make it Credible and Efficient, Doctoral Dissertation, Royal Institute of Technology, Stockholm, Sweden.

Jones, A. and Ashenden, D. (2005). http://issj.sys-con.com/author/ashenden.htm, Accessed: 25/03/05.

Jonsson, E. (1995). A Quantitative Approach to Computer Security from a Dependability Perspective, Doctoral Dissertation, Department of Computer Engineering, Chalmers University of Technology, Gothenburg, Sweden.

Kaarst-Brown, M.L., and Kelly, S. (2005). IT Governance and Sarbanes-Oxley: The Latest Sales Pitch or Real Challenges for the IT Function? Proceedings of the 38th Hawaii International Conference on Systems Sciences.

Kaarst-Brown, M.L., and Robey, D. (1999). More on Myth, Magic and Metaphor: Cultural Insights into the Management of Information Technology in Organizations, Information Technology and People, 2(2): pp. 192-217.

Kaen, F.R. (2003). A Blueprint for Corporate Governance, American Management Association.

Kahn, D.A. (1996). The Codebreakers: the Story of Secret Writing. Scribner, New York.

Kaplan, B. and Duchon, D. (1988). Computing Qualitative and Quantitative methods in Information Systems Research: A Case Study, MIS Quarterly 12(4). pp.571-586.

Katz, D. M. (2006). Sarbox Takes a Constitutional, CIO.com, Accessed: 23/09/08.

Keen, P.G. W. (1991). Relevance and Rigor in Information Systems Research: Improving Quality, Confidence, Cohesion and Impact, In Information Systems Research: Contemporary Approaches and Emergent Traditions, (Eds. Nissen H-E, Klein H.K and Hirschheim R), IFIP, Norht-Holland, pp. 27-49.

Keen, P.G.W, Ballance, C, Chan, S. and Schrump, S. (2000). Electronic Commerce Relationships – Trust by Design, Prentice-Hall, Upper Saddle River, NJ, USA.

Kimble, C. and Hildreth, P. (2004). Communities of Practice: Going One Step Too Far? Proceedings 9e Colloque de l'AIM, Evry, France.

Klein, H. and Lyytinen, K. (1985). The Poverty of Scientism in Information Systems. Proceedings of the IFIP WG 8.2. Working Conference on Research Methods in Information Systems. Elsevier Science Publisher, Amsterdam, pp. 131-161.

Land, F. F. and Kennedy-McGregor, M. (1987). Information and Information Systems: Concepts and Perspectives. In Information Analysis: Selected Readings (Galliers R.D., Edition), Wokingham: Addison-Wesley.

LeBon, G. (1896). The Psychology of Socialism. Kessinger Publishing. ISBN 1432528238

Lee, A.S. (1989). A Scientific Methodology for MIS Case Studies, MIS Quarterly, 13(1): pp. 32-50.

Lee, A.S. (1991). Integrating Positivist and Interpretive Approaches to Organizational Research, Organization Science, 2(4), pp.342-365.

Lee, A.S., Liebenau, J. and DeGross, J.I. (1997). Information Systems and Qualitative Research, Chapman and Hall, London.

Lehaney, B. Clarke, S. Coakes, E. and Jack, G. (2004). Beyond Knowledge Management, Idea Group Publishing, London.

Leidner, D. and Kayworth T. (2006). Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict, MIS Quarterly, 30(2): pp. 357-399.

Lemon, M. and Sahota, P. (2004). Organisational Culture as a Knowledge Repository for Increased Innovative Capacity, Technovation, 24, pp.483-498.
Levin, W., (1988). Sociological Ideas: Concepts and Applications, Wadsworth.
Levitt, B. and J. March (1988). Organizational Learning, Annual Review, of Sociology, 14, pp.319-340
Liebenau, J. and Backhouse, J. (1990). Understanding Information. London, Macmillan.
Liebowitz, J. and Chen, Y. (2003). Knowledge Sharing Proficiencies: The Key to Knowledge Management, in Holsapple, C.W. (Edition), Handbook on Knowledge Management 1: Knowledge Matters, Springer-Verlag, Berlin, pp. 409-24.
Lievesly, S. (1995). Security into the 21st Century. The Risk and Security Management Forum, Police Staff College, Bramshill.
Lillis A.M. and Mundy J. (2005). Cross-Sectional Field Studies in Management Accounting Research - Closing the Gaps between Surveys and Case Studies, Journal of Accounting Management Research, 17: pp. 119–141.
Lincoln, Y.S. and Guba, E.G. (1985). Naturalistic Inquiry. Sage, Beverly Hills, CA.
Lucas, Jr,H. (1991). Commentary in the Information Systems Research Challenge: Survey Research Methods, in Kraemer, K., Cash J. and Nunamaker, J.F. (Edition), Harvard Business Press, pp. 67-79.
Malhorta, Y. (2000). Knowledge Management and Virtual Organisations, Idea Group Publishing, London.
Manunta, G. (2000). Defining Security. Diogenes Paper No.1. Cranfield Security Centre, RMCS, Shrivenham.
Marin, A. (1992). Cost and Benefits of Risk Reduction. In Risk: Analysis, Perception and Management. London: Royal Society.
Marshall, C., Rossman, B.G. (1989). Designing Qualitative Research, Sage Publications, Inc., Newbury Park, CA.
Mattia, A., and Dhillon, G. (2003). Applying Double Learning to Interpret Implications for Information Systems Security Design. IEEE Systems, Man and Cybernetics Conference, Washington DC.
Maturana, H.R. and Varela, F.J. (1998). The Tree of Knowledge, Shambala, Boston, MA/London.
McGrath, J.E. (1984). Groups: Interaction and Performance, Prentice Hall, Eaglewood Cliffs, N.J.
Menezes, A.J, Van Oorschot, P.C. and Vanstone, S.C. (1999). Handbook of Applied Cryptography. CRC Press, Boca Raton, FL.
Miles, M.B., and Huberman, M.A. (1994). An Expanded Sourcebook of Qualitative Data Analysis, Sage Publications, California.
Mishra, S. and Dhillon, G. (2008). The Impact of the Sarbanes-Oxley (SOX) Act on Information Security, Information Security and Ethics: Concepts, Methodologies, Tools, and Applications, pp.1-21.
Moulton, R. and Coles, R.S. (2003). Applying Information Security Governance, Computers and Security, 22(7): pp.580-584, 0167-4048/03, Elsevier Ltd.
Mumford, E. (1985). Researching People Problems: Some Advice to a Student, in Mumford, E., Hirschheim, R., Fitzgerald, G., Wood-Harper, A. (Editors), Research Methods in Information Systems, Elsevier Science Publishers, North Holland, pp. 315-320.
Nazareth, A. (2006). Keeping SarbOx is Crucial, in Business Week, (4009): pp. 134-134.
Neumann, P. (1995). Computer Related Risks, New York: ACM Press, pp. 203-304.
Nissen, H. (1985). Acquiring Knowledge of Information Systems: Research in a Methodological Quagmire, in Mumford, E., Hirschheim, R., Fitzgerald, G.,

Wood-Harper, A., (Editors), Research Methods in Information Systems (Elsevier Science Publishers, North Holland), pp. 39-51.
Nonaka, I. (1994). A Dynamic Theory of Organisational Knowledge Creation, Organisation Science, 5(1): pp.14-37.
Nonaka, I. and Takecuchi, H. (1995). The Knowledge Creating Company, Oxford Press, Oxford, England.
Nutt, P.C. (1984). Types of organizational decision processes, Administrative Science Quarterly, 29: pp.414-450.
O'Dell, C., Elliot, S. and Hubert, C. (2004). Achieving Knowledge Management Outcomes, in Holsapple, C, Handbook on Knowledge Management, 2nd Edition, pp. 253-287.
Olaisen, J.L. (1991). Pluralism or Positivistic Trivialism Important Trends in Contemporary Philosophy of Science. In Nissen H., Klein H.K. and Hirschheim R. (Eds), Information Systems Research: Contemporary Approaches and Emergent Traditions, Proceedings of the IFIP TC8/WG 8.2 Working Conference, Elsevier Science Publishers B.V. (North-Holland), pp. 235-266.
Oppong, S. A., Yen, D.C. and Merhout, J.W., (2005). A New Strategy for Harnessing Knowledge Management in E-commerce, Technology in Society, 27, pp. 413-435.
Orlikowski, W. (2002). Knowing in Practice: Enacting a Collective Capability in Distributed Organizing, Organization Science, 13(3): pp.249-273.
Orlikowski, W.J. (1993). CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development, MIS Quarterly, 17(3): pp.309-340.
Orlikowski, W.J., and Baroudi J.J. (1991). Studying Information Technology in Organisations: Research Approaches and Assumptions, Information Systems Research, 2(1): pp. 1-28.
Pabrai, U. (2005). Wireless Security, HIPAA Academy, http://www.hipaaacademy.net/pdf/WirelessSecurityWP.pdf, Accessed: 30/03/2005.
Pan, S. and Leidner, D. (2003). Bridging Communities of Practice with Information Technology in Pursuit of Global Knowledge Sharing, Journal of Strategic Information Systems, 12: pp.71-88
Parker, D. (1991). Seventeen Information Systems Myths Debunked, In K. Dittrich, S.Rautakivi, and J.Saari, eds., Computer Security and Information Integrity. Amsterdam: Elsevier Science Publishers, pp. 363-370.
Parker, D.B. (1981). Computer Security Management, Prentice Hall, Reston, USA.
Parker, D.B. (1998). Fighting Computer Crime - a New Framework for Protecting Information. Wiley Computer Publishing, New York.
Patterson, T. (2005). Mapping Security: The Corporate Security Sourcebook for Today's Global Economy, Published Dec 14, 2004 by Addison-Wesley Professional. Part of the Symantec Press series.
Patton, M.Q. (1990). Qualitative Evaluation and Research Methods, 2nd Edition, Newbury Park, CA: Sage Publications.
Peterson, L.L., and Davie, B.S., (1996). Computer Networks: A Systems Approach, Morgan Kaufmann Publishers.
Pettigrew, A. M. (1979). On Studying Organizational Cultures, Academy of Management Review [AMR], 24: pp. 570-581.
Polanyi, M. (1966). The Tacit Dimension, First Edition, Anchor Books, New York.
Polanyi, M., (1975). Personal Knowledge. In M. Polanyi and H. Prosch (Edition). Meaning, University of Chicago Press, Chicago.

Poole, V. (2001). Assessing the European IT Governance Climate, Information Systems Control Journal, 2(1).
Post, R.S. and Kingsbury, A.A. (1991). Security Administration: An Introduction to the Protective Services. Butterworth-Heinemann, London.
Prusak, L. (2001). Where Did Knowledge Management Come From? IBM Systems Journal, 40(4): pp. 1002.
Pugh, D.S., Hickson, D.J., and Hinings, C.R. (1983). Writers on Organisations (3rd Edition). Penguin Books Ltd., Harmondsworth, Middlesex, England.
Raghu, T.S. and Vinze, A. (2005). A Business Process Context for Knowledge Management, Decision Support Systems, 43: pp. 1062-1079.
Ramos, D., (2001). The Auditors Role in IT Governance, Information Systems Control Journal, 5: pp. 23-24.
Randeree, E. (2006). Knowledge Management: securing the future, Journal of Knowledge Management, 10(4), pp. 145-156, Emerald Group Publishing Limited, ISSN 1367-3270.
Ravenel, J. (2006). Effective Operational Security Metrics, Information Systems Security, 15(3): pp. 10-17.
Remenyi, D. (1998). Doing Research in Business and Management: An Introduction to Process and Method, Sage Publications, London.
Remenyi, D., and Williams, B. (1995). Some Aspects of Methodology for Research in Information Systems, Journal of Information Technology 10: pp.191-201.
Reynolds, C. (2003). Undergraduate Information Assurance Curriculum. Proceedings of the 2003 Workshop on Information Assurance, pp. 10-16.
Rittenberg, L.E. and Senn, A. (1993). End-user Computing—Is it True that End-user Computing is like a Runaway Train? Internal Auditor February: pp. 35–39.
Roberts, J. (2006). Limits to Communities of Practice. Journal of Management Studies, 43(3): pp. 623–63.
Robson, C. (1993). Real World Research: A Research for Social Scientist and Practitioner-researchers, Oxford, Blackwell.
Robson, C. (2002). Real World Research (2nd Edition), Oxford, Blackwell.
Ruppel, C.P. and Harrington, S.J. (2001). Sharing Knowledge through Intranets: A Study of Organisational Culture and Intranet Implementation, IEEE Transactions on Professional Communication, 44(1): pp.37-52.
Rutkowski, M. (1999). Two Perspectives on Knowledge Transfer, http://www.walshcol.edu/mrutkow/knowledgeA.htm, Accessed: 23/01/2007.
Saint-Onge, H. (1996). Tacit Knowledge: The Key to the Strategic Alignment of Intellectual Capital. Strategy & Leadership March/April, 10-14.
Saunders, M., Lewis, P. and Thornhill, A. (2003). Research Methods for Business Students, 3rd Edition, Prentice Hall, pp. 327-374.
Schein, E. H. (1985a). How Culture Forms, Develops and Changes, in Gaining Control of the Corporate Culture, R.H. Kilmann, M.J. Saxton, R. Serpa, and Associates (eds.), Jossey-Bass, San Francisco, pp.17-43.
Schein, E. H. (1985b). Organizational Culture and Leadership, San Francisco: Jossey-Bass.
Schon, D.A. (1983), The Reflective Practitioner. Basic Books, New York.
Siponen M. and Willison R (2007). A Critical Assessment of IS Security Research between 1990-2004. In Proceedings of the Fifteenth European Conference on Information Systems (Österle H, Schelp J, Winter R Edition), pp. 1551-1559, University of St. Gallen, St. Gallen.
Siponen, M. (2000). A Conceptual Foundation for Organizational Information Security Awareness, Information Management and Computer Security, 8: pp.31-41.

Siponen, M. and Iivari, J. (2006). Six Design Theories for IS Security Policies and Guidelines, Journal of the Association for Information Systems, 7(7): pp. 445-472.

Siponen, M., Willison, R. and Baskerville, R. (2008). Power and Practice in Information Systems Security Research, in the Proceedings of the Twenty Ninth International Conference on Information Systems.

Siponen, M.T. (2005). An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice, European Journal of Information Systems, 14(3): pp. 303-315.

Smith, H.A., and McKeen, J.D. (2004). Valuing the Knowledge Management Function, in Holsapple, Handbook on Knowledge Management, 2 Knowledge Directions, 2nd Edition, pp.353-368.

Smith, H.J., and Hasnas, J. (1999). Ethics and Information Systems: The Corporate Domain, MIS Quarterly, 23(1): pp.109-127.

Soo, C., Devinney, T., Midgley, D. and Deering, A., (2002). Knowledge Management: Philosophy, Processes, and Pitfalls. California Management Review, 44(4): pp.129-150.

Spagnoletti, P. and Resca, A. (2007). A Framework for Managing Predictable and Unpredictable Threats: The Duality of Information Security Management. In Proceedings of the Fifteenth European Conference on Information Systems (Österle H, Schelp J, Winter R Edition), pp.1539-1550, University of St. Gallen, St. Gallen.

SSE-CMM (1998a). The Model V2.0. Http://www.sse-cmm.org, Accessed: 12/02/2006.

SSE-CMM (1998b). The Appraisal Method V2.0. Http://www.sse-cmm.org, Accessed: 12/02/08

Stake, R. (1978). The Case Study Method in Social Inquiry, Education Research, 7: pp.5-8.

Stake, R.E. (1994). Case Studies. In N.K. Denzin and Y.S. Lincoln (Edition), Handbook of Qualitative Research, Sage Publications Inc., pp. 236-247.

Stallings, W. (2001). Operating Systems, Fourth Edition, Prentice Hall.

Stamper, R.K. (1973). Information in Business and Administrative Systems. New York: John Wiley and Sons.

Standards Australia. (2001). HB275-2001, Knowledge Management: A Framework for Success in the Knowledge Era, Sydney, NSW: Standards Australia International Limited.

Stevens, B. and Brownell, J. (2000). Ethics: Communicating Standards and Influencing Behavior. Cornell Hotel and Restaurant Administration Quarterly, 41: pp.39-43.

Stewart, A. (2005). Information Security Technologies as a Commodity Input, Information Management and Computer Security, 13(1).

Stewart, T.A., (1997). Intellectual Capital: The New Wealth of Organisations, First Edition, New York: Doubleday.

Stone, E. (1978). Research Methods and Philosophy of Science, in Organizational Behaviour, S. Kiev (Ed.), Columbus, Ohio, pp.15-40.

Stoneburner, G., Goguen, A., and Feringa, A. (2002). Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, Publication 800-30, pp. 1-54.

Strassman, P.A (1995). Reengineering, Excerpted from The Politics of Information Management, The Information Economics Press.

Straub, D., Goodman, S., and Baskerville, R. (2008). Framing of Information Security Policies and Practices, in Information Security Policies, Processes, and Practices, D. Straub, S. Goodman and R. Baskerville (Edition), Armonk, NY: M. E. Sharpe.

Straub, D.W and Welke, R.J (1998). Coping with Systems Risk: Security Planning Models for Management Decision-making, MIS Quarterly, 22: pp.441-464.
Strauss, A., and Corbin, J. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques, Newbury Park, CA: Sage Publications, Inc.
Sundt, C. (2006). Information Security and the Law, Information Security Technical Report, 11: pp. 2-9.
Sveiby, K. and Simons, R. (2002) Collaborative Climate and Effectiveness of Knowledge Work—an Empirical Study, Journal of Knowledge Management, 6(5): pp.420-433.
Tesch, R. (1990). Qualitative Research: Analysis Types and Software Tools. New York, Falmer.
Thomson, M. E. and Von Solms, R. (1998). Information Security Awareness: Educating Your Users Effectively. Information Management Computer Security 6(4): pp. 167-173.
Tiwana, A. (2000). The Knowledge Management Toolkit, Upper Saddle River, NJ, Prentice Hall.
Tolsby, J. (1998). Effects of Organizational Culture on a Large Scale IT Introduction Effort: A Case Study of the Norwegian Army's EDBLF Project, European Journal of Information Systems, 7(2): pp.108-14.
Trompeter C, and Eloff, J. (2001). A Framework for the Implementation of Socio-ethical Controls in Information Security. Computers and Security, 20(5): 384e91.
Truex, D.P. and Baskerville, R. (1998). Deep Structure or Emergence Theory: Contrasting Theoretical Foundation for Information Systems Development. Information Systems Journal, 8(2): pp. 99-118.
Tsohou, A., Theoharidou,A., Kokolakis1,S. and Gritzalis, D. (2006).Addressing Cultural Dissimilarity in the Information Security Management Outsourcing Relationship, C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.): TrustBus, LNCS 4657, pp. 24–33, Springer-Verlag Berlin Heidelberg.
Tyndale, P. (2002). A Taxonomy of Knowledge Management Software Tools: Origins and Applications, Evaluation and Program Planning, 25: pp.183-190.
Ulrich, D., and N. Smallwood (2004). Capitalizing on Capabilities, Harvard Business Review, 82(6): pp.119–127.
URN 96/702. (1996). The Business Manager's Guide to Information Security, Department of Trade and Industry, London.
Van Maanen, J., Dabbs, J.M., and Faulkner, R.R. (1982). Varieties of Qualitative Research. Beverly Hills, CA: Sage Publications.
Veriscan (2006). Veriscan Security A.B, Karlstad, Sweden, www.veriscan.net, Accessed: 23/01/08
Villarroel, R., Fernández-Medina, E. and Piattini, M., (2005). Secure Information Systems Development – A Survey and Comparison, Computers and Security, 24(4): pp.308-321.
Von Solms B. and Von Solms R. (2004). The Ten Deadly Sins of Information Security Management, Computers and Security, 23(5): pp.371–6.
Von Solms, B. (2001). Corporate Governance and Information Security, Computers and Security, 20 (3): pp. 215-218.
Von Solms, R. (1999). Information Security Management: Why Standards are Important, Information Management and Computer Security, 7: pp.50-58.
Vroom, C. and Von Solms, R. (2004). Towards Information Security Behavioural Compliance, Computers and Security, 23(3), pp.191-198.
Walsham, G. (1993). Interpreting Information Systems in Organizations, John Wiley and Sons, Chichester, UK.

Walsham, G. (1995). Interpretative Case Studies in IS Research: Nature and Method. European Journal of Information Systems, 4(2): pp.74-81.
Walsham, G. (2001). Knowledge Management: the Benefits and Limitations of Computer Systems. European Management Journal, 19(6): pp.599-608
Walsham, G. and Sahay, S. (1999). GIS for District-level Administration in India: Problems and Opportunities, MIS Quarterly, 23(1): pp.39-66.
Wang, J., Chaudhury, A. and Rao, H.R. (2008). A Value-at-Risk Approach to Information Security Investment, Information Systems Research, 19(1): 106-120.
Webster, J., and Watson, T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review, MIS Quarterly 26(2): pp. 13-23.
Wenger, E. (2000). Communities of Practice and Social Learning Systems, Organization, 7(2): pp.225–46.
Wenger, E. and Snyder, W. (2000). Communities of Practice: the Organizational Frontier, Harvard Business Review, Jan–Feb: pp.139–45.
Wenger, E., McDermott, R., Snyder, W.M. (2002). Cultivating Communities of Practice. Harvard Business Press; 1st Edition. ISBN 978-1578513307.
Whitman, M. (2003). Enemy at the Gates: Threats to Information Security, Communications of the ACM, 46(8): pp.91-95.
Whitman, M. (2004). In Defence of the Realm: Understanding the Threats to Information Security, International Journal of Information Management, 24(1): pp.43-57.
Whitman, M.E. and Mattord, H. J., (2005) Readings and Cases in the Management of Information Security, Course Technology, Boston, MA, ISBN 0-619-21627-1
Wiant, T.L. (2005). Information Security Policy's Impact on Reporting Security Incidents, Computers and Security, 24 (10): pp.448-459.
Wickramasinghe, N. (2003). Do We Practise What We Preach: Are Knowledge Management Systems in Practice Truly Reflective of Knowledge Management Systems in Theory?, Business Process Management Journal, 9(3): pp. 295–316.
Widener, S. K., and F. H. Selto. (1999). Management Control Systems and Boundaries of the Firm: Why do Firms Outsource Internal Auditing Activities? Journal of Management Accounting Research, 11 (Fall): pp.45–73.
Wiig, K. (1999). Introducing Knowledge Management into the Enterprise, in Knowledge Management Handbook, CRC Press, Boca Raton, FL, 3-1-41.
Williams, C.A., Jr, Smith, M.I. and Young, P.C. (1995). Risk Management and Insurance (7th Edition). McGraw-Hill, New York.
Willison, R. and Backhouse, J. (2006). Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective, European Journal of Information Systems, 15: pp. 403-414.
Wiseman, C. (1988). Strategic Information Systems, Irwin, Homewood, IL.
Wong, K. Y., and Aspinwall, E. (2005). Development of a Knowledge Management Initiative and System: A Case Study, Expert Systems with Applications, pp.1-9, Elsevier.
Wood, C. (1999). Information Security Policies Made Easy, Baseline Software, San Rafael, CA.
Wood, C. (2001). Information Security Policies Made Easy, Publisher: InfoSecurity Infrastructure, 2001), ISBN-13: 978-1881585077.
Wrapp, H.E, (1991). Good Managers Don't Make Policy Decisions, In H.Mintzberg and J.B. Quinn (Edition), The Strategy Process, Englewood Cliffs, NJ: Prentice-Hall: pp.32-38.
Yin, R. K. (1994). Case Study Research, Design and Methods (2nd Edition.), Newbury Park, CA, Sage Publications.

Yin, R.K. (1989). Case Study Research – Design and Methods, Applied Social Research Methods Series (Ed. 1), 5, Sage Publications, CA.
Yin, R.K. (2003). Case Study Research: Design and Method, Sage Publications Inc., Thousand Oaks, CA.
Yin, R.K., (1984). Case Study Research – Design and Methods, Applied Social Research Methods Series, Sage Publications, 5: pp.13 – 150.
Zeide, J.S. and Liebowitz, J. (1987). Using Expert Systems: The legal Perspective, IEEE Expert, 2(1): pp. 19-21.

APPENDICES

Appendix A: Sphere of Security

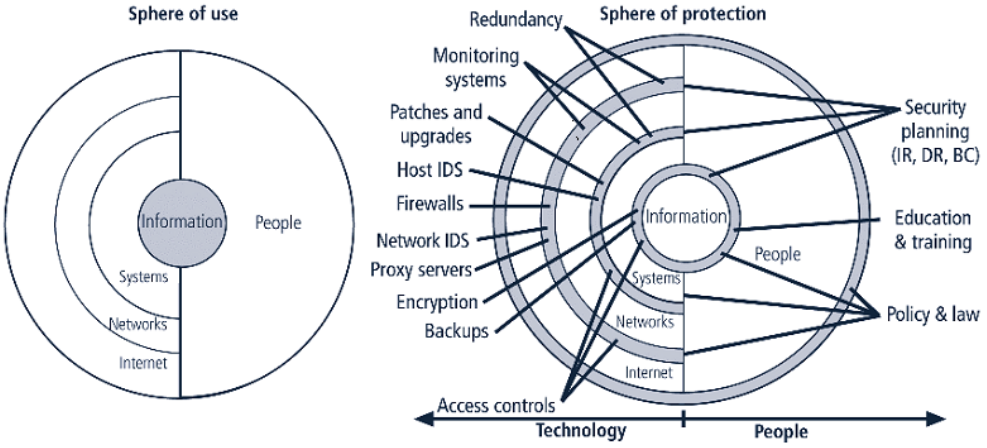

Figure 1: Sphere of Security (Source: Whitman & Mattord, 2005, p.198).

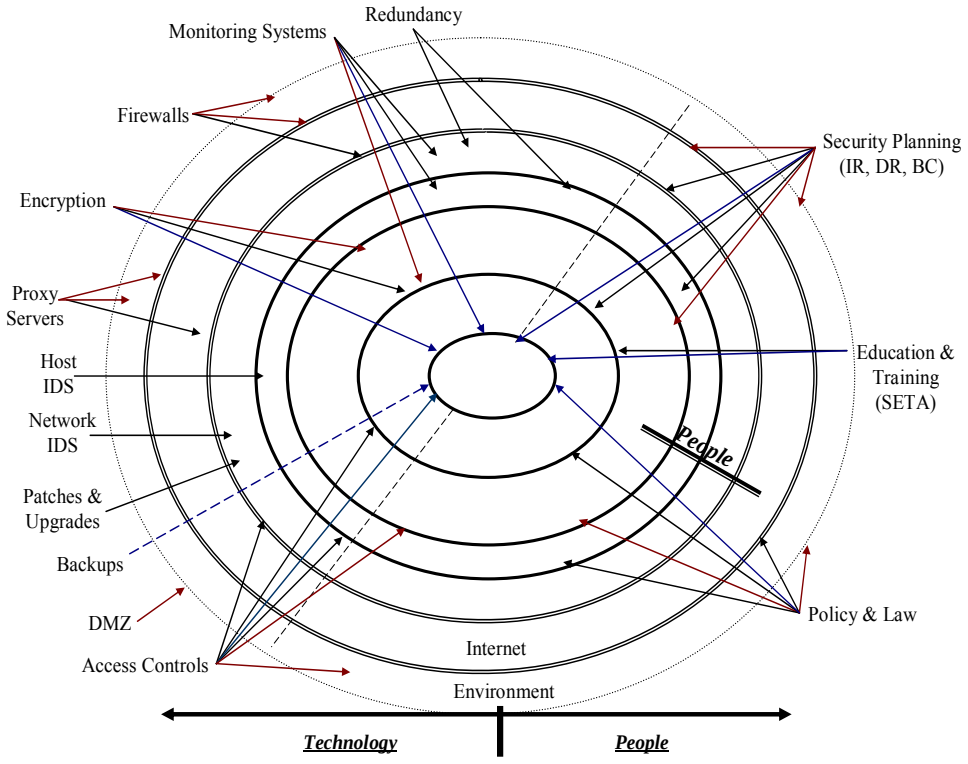

Figure 2.2: Proposed Countermeasures for data, information and knowledge (Adapted by the Researcher from Whitman & Mattord, 2005, p.198, Appendix A).

Appendix B: Interview Guide

1. Determine the type of Organisational infrastructure used in the case study
Identify the type(s) of Culture, common knowledge, Structure and communities of practice used in IIS or CS Identify any barriers that may exist in terms of the above Identify the type of physical environment the functions operate in and the restrictions caused How is it arranged from and across the different sites? Identify the IT infrastructure used to support the needs of the functions
2. Determine the type and role of the ISS or CS knowledge used:
General Knowledge |Technical Knowledge| Contextual Knowledge -Display matrices were used to verify the types and roles of knowledge in supplementary interviews.
3. Determine where ISS or CS knowledge is located
Identify the knowledge stores or reservoirs used by the ISS or CS functions Individuals, Groups, Procedures, Repositories, Technologies, Organisation, Units, Inter-organisational Relationships -Display matrices were used to verify the knowledge reservoirs identified in supplementary interviews.
4. Determine the types of processes used by ISS and CS
Identify how the functions acquire, capture, create, Share, apply and control their knowledge -Display matrices were used to verify the knowledge processes identified in supplementary interviews.
5. Determine the impact of managing ISS or CS knowledge
Identify the impacts on Individual employees, the function, the organisation -Display matrices were used to verify the impacts identified in supplementary interviews.
6. Determine how the organisation aligns Knowledge Management with security and how is the impact of one on the other assessed.
Identify the main business functions of the business Identify the value chain processes of the organisation? What are the main cross-functional business processes of the organisation? Identify the inter & intra-organisational alliances and contributions? How is quality measured? The main information systems supporting individual / group/ business needs Culture of the organisation in promoting: Knowledge Management/ Security |Inter / intra collaboration | Continuous Improvement (TQM) Innovative | Evaluate the value of the information / knowledge for Org & Group Outline a map of knowledge and security within the organisation: Teams, Systems, Repositories | Knowledge Resources (Experts) Knowledge Assets – Org, Dept & Individual Level Knowledge Structures – Knowledge Domain Knowledge Applications – Problem-solving (People, Docs, DB) Knowledge Developments – progression (Learning Org.)
7. Determine how the organisation strikes a delicate balance between a secure and a productive (Knowledge Sharing) environment.
Employees responsible for Knowledge in the organisation Roles in the department: Knowledge Manager, Knowledge group How many employees are in the knowledge group? What is the staff turnover? Experts – How can you ensure that their expertise is retained? How is knowledge shared between experts? Mentoring | On the job experience | Training Email – Problem & Solution, minutes of meetings, lessons-learned Knowledge Managers | Investment in KM / Security over the last: 1yr, 2yrs, 5yrs, 10yrs Establish the assessment of the contribution of KM / Security to the organisation

Roles in the IS department: IT Manager; Security Officer; Security Group; Outline the map of security within the organisation Experts – How can you ensure that their expertise is retained? How is knowledge shared between experts? Email – Problem & Solution, minutes of meetings, lessons-learned Intranet – Knowledge web Do you agree that the same knowledge tools that make security workers more productive and additionally make attackers more powerful? Tools used to share knowledge: Extranets, Access control mgt, Knowledge Portals 1yr, 2yrs, 5yrs, 10yrs How do you assess the contribution of security to the organisation? What is your company's biggest security threat? What is your biggest IT security concern?
8. Establish end-users impact on knowledge sharing and how can these impacts be minimised through appropriate security administration.
Employee motivation to share and protect knowledge Knowledge Management Issues-customer: Who can access what? What information / knowledge do users need to do their work? Can groups of users be defined, who accesses the same information? What do users want information / knowledge for? How is information / knowledge shared between groups of users? How is information / knowledge input, stored, accessed and transmitted between users? Is data stored or transmitted in a form accessible by non-authorised users? Where are the "nodes" that data passes consistently? How can the different forms of data be made compatible? Supply/Security Issues: Is the information / knowledge supplier trustworthy? Can external as well as internal information / knowledge be collected
9. Determine the key threats and defences against both internal and external security abuse.
Determine the company's biggest threat to KM Types of breaches of security faced and the consequences to KM Does your company have an incident response plan? How do you perform security checks on your partners? What level of control do you give your partners? What technologies are used for access control? How do you ensure that they can only access the information that they should have access to? How is Access Control controlled? Do you have centralised access control? Is it at your ideal level? How many applications are integrated?
10. Determine the impact of changing organisational structures on Knowledge Management / IS Security, (for e.g.: in supporting geographically dispersed offices).
Determine if the contribution of collaboration to the organisation is assessed. Experienced/ suspected a security threat (and loss of Knowledge) due to a competitor. Measure the level of risk against the benefit of openness (for customers and trading partners Tracking users and what they are permitted to do
11. Determine the impact of changing organisational structures on Knowledge Management / Security, (for e.g.: in supporting geographically dispersed offices).
Identify problems in managing knowledge across the different subsidiaries Identify the difficulty in securing a multinational organisation

The Interview Guide, shown above, was altered for each of the three groups of interviewees outlined in Chapter 3, Table 3.3

Appendix C: CME-Co ISS Knowledge & TELE-Co ISS Knowledge

CME-Co AND TELE-Co IS SECURITY FUNCTIONAL KNOWLEDGE											
D:E/T |P:E/T		**CME-Co: IS SECURITY KNOWLEDGE**	**Role**				**TELE-Co: IS SECURITY KNOWLEDGE**	**Role**			
General Knowledge	D:E	Org. Doc.| Vendor /Internal Warnings| Threats.	O			D:E	Org. Documentation| Charts| Contacts	O		
	D:E	HW/SW Specifications: Firewalls| Servers.	O			D:E	Security HW Lists| Template	O		
	D:T	Regulations| Impact of Threats| Roles: Escalations	O			D:T	Regulations| Technology| System| Threats| Roles	O		
	D:T					D:T	Networks| Domains| Procedures	O		
	P:E	Procedures| White Papers – Projects ISS Issues.	O			P:E	Checklists| Policies	O		
	P:T	Steps to Align IT & Access Control Lists (ACL)	O			P:T	ID Assets| Assessment Criteria	O		
			O	**T**	**S**			**O**	**T**	**S**
			11	0	0			15	0	0
Technically Specific	D:E	IS Security Policy| Strategy| Regulations	S			D:E	ISS Policy| Strategy| Regulations	S		
	D:E	ACL & Alert Reports from Security Technologies.	O			D:E	Audit| Alert & Evaluation Report	O		
	D:T	Domain Access Rights: Segregation of Duties.	O			D:T	Domain Access Rights	O		
	D:T	Implement Regulations| Systems| Risk Knowledge.	T			D:T	Controls| Scanning| Forums	T		
	D:T	Advising Customers: ISS Issues & Tools	S			D:T	Evaluation of Technologies	S		
	P:E	Standards & Procedures.	T			P:E	ISO17799 | Trouble-shooting	O		
	P:T	Developing Plan & Strategy| Security Methods.	S			P:T	Audit Reviews| Best Practices	T		
	P:T					P:T	Prioritise Vulnerabilities	O		
			O	**T**	**S**			**O**	**T**	**S**
		Totals:	4	6	5		**Totals:**	7	5	3
Contextually Specific	D:E	SOX Requirements| Risk Criteria| Manuals	O			D:E	Regulations| Standards| Practices| Alerts	O		
	D:E	Audit Reports: Evaluation Feedback| NW Testing	T			D:E	IS Security Audit Reviews	T		
	D:T	ISS Specialists Knowledge of: SOX| Risks| Audits	T			D:T	SOX| Impact of Technologies	O		
	D:T					D:T	Regulations| Practices| Risks| Controls	T		
	P:E	ISS Teams: Steps for Standards| Review	T			P:E	Steps: Lessons-learned| Audits	T		
	P:T	ISS Officers: Steps for: Incidents| Audits	T			P:T	Steps: Identify & React to Rogues	T		
			O	**T**	**S**			**O**	**T**	**S**
		Totals:	5	9	0		**Totals:**	5	9	0
		ISS Knowledge Totals	**28**	**20**	**15**		**ISS Knowledge Totals**	**27**	**14**	**3**

***Declarative (D)/ Procedural (P), Explicit (E)/ Tacit (T). \| *Roles: Operational (O), Tactical (T) Strategic (S).**
***Totals are calculated from Tables: CME-Co ISS Knowledge & TELE-Co ISS Knowledge (Source: Adapted from Tables 5.4 & 6.4)**

Appendix D: CME-Co IS Security and Customer Support Reservoirs

Knowledge Stores	ISS AND CS FUNCTIONAL RESERVOIRS OF KNOWLEDGE		CHARACTERISTICS OF KNOWLEDGE RESERVOIRS
	IS SECURITY RESERVOIRS	**CUSTOMER SUPPORT RESERVOIRS**	
(1.) Individuals	➢ ISS Specialists: Engaged in Problem-solving ➢ Engineers: Creating Security enhancements ❖ GIS Director: Purchasing & Customising Best Practices ❖ Site Security Officer: Implementing Controls ❖ Corp. Sec. Officer: Identifies Stakeholder requirements ❖ Auditor: Evaluates the ISS Controls used ❖ OISRM Coordinator: Source Regulatory Guidelines	➢ CS Specialists: Engaged in Problem-solving ➢ Engineers: Creating Product Designs| Fixes ▪ CS Manager: Coordinating CS ▪ Knowledge Consultant: Centralising Knowledge ▪ KDG Officer: Develops & Coordinates Training ▪ Knowledge Champion: Promotes KM Practices ▪ Level (1|2) Technicians: Provide 1st & 2nd Support	✣ Escalated levels of Expertise ✣ Solution / Product Innovators ✣ Senior Role: steering (ISS) practices ✣ Global Coordinators: implementing controls ✣ Stakeholder Analyst: identifying requirements ✣ In/External Evaluator: assessing ISS ✣ KM Champion: promoting training| consolidation of (ISS) knowledge
Differences	o Engineers enhance existing products with Security tools o Formal Senior GIS Security Role to promote ISS o Site Coordinators oversee global rollouts (e.g. patches) o Stakeholder (Customer) identifies market requirements o Auditor performs an external review |measure	o CS Manager controls international operations o Knowledge Consultant consolidates CS knowledge o KDG Officer provides Technician training o Knowledge Champion promotes KM within CS o Technicians provide front-line Customer support	
(2.) Groups	➢ Management: Enforces Standards & Procedures ➢ Security Officers: Utilise Domain & Control Knowledge ➢ GIS|IT Departments: Provide IT Services & Guidelines ❖ OISRM: Provide a Pool of Regulatory Experts ❖ Corporate Security: Strategies & Development ❖ Internal Audit Committee: Compliance issues| reviews ❖ Remote Services: External Access Requirements	➢ Managerial Forum: Define Policies ➢ CS Engineers: Support Product Portfolio| Diagnose ➢ Engineering: Develop Products & Provide Support ▪ KDG CS Group: KM Strategy for CS ▪ KCS (Centred Support) CoP: Review Solutions	✣ Managerial Responsibility: policies| standards ✣ Specialised (ISS) Support Teams: diagnosing problems| applying controls ✣ Corp. (ISS) Group: providing specialised knowledge on regulations| strategies| audits| domain knowledge ✣ Quality Assessors: solutions| reviews| standards| post-mortems| training needs ✣ Centralised IT | ISS Services: rollouts of technical controls & patches ✣ Evaluation Group: measuring value ✣ Communication Group: establishing secure in/external connections
Differences	o Two (Official) Security Groups: Regulatory Standards & Stakeholder Groups o Compliance is assured & product enhancements made o Evaluation Group provide a form of measurement o Secure external (Partner) connections are monitored	o Ad hoc groups are used to support & promote KM o Levels of escalation are defined & use measured (costing) o Group created to develop CS skills o Collaborate with & support Sales | EBC o Quality review process used to assess solutions by a CoP	
(3.) Procedures	❖ Compliance Procedures: Customised to U.S| International ❖ M-Gates Method: Used to Manage Projects ❖ Checklists: Outline ISS Activities to be completed ❖ Six Sigma: Case Template for Resource Allocation	▪ Templates: Used for Creating Solutions & CBR Searches ▪ Call Escalation Procedures: Used to Control the Problem-solving Process to Measure Costs.	✣ Templates: quality solutions| tagged for CBR searches ✣ Procedures: in/external control| environmental standards| problem-solving escalations ✣ Checklists: prioritise activities ✣ Project Management Methodology: collaboration across teams ✣ Resource Allocation Method: budgetary restriction
Differences	o Procedures are externally sourced o Project management methodology is used o ISS activities are listed & completed (e.g. for a review) o Resources allocation procedures for shared resources	o Templates for solution are used to ensure quality & reuse o Levels of expertise are identified, formally documented & assigned to: problems| products| code	
	➢ Document Mgt. System: Stores Solutions & Guides	➢ Document Mgt. System: Stores Solutions &	✣ Documentation Management System:

(4.) Repositories	➢ Intranet: Centralises Common & Group Knowledge ➢ Vendor Repositories: Used to Source Manuals, Guides ➢ Knowledge-Link (University): Provides Online Training ➢ Desktops: Store Individual Doc., Solutions & Guides ➢ Portals (E-Room| Power-Link): Used for Collaboration ➢ Email Alerts: Notification of for e.g. New Threats ❖ Global Tech Web: Accessed for Patches & Solutions ❖ Q &A Repositories| Forums: Query Ex/Internal Experts ❖ Shared Drives: Store Solutions & Procedures	Guides ➢ Intranet: Corp. Info. & Group websites ➢ Vendor Repositories: Used to Source Manuals, Guides Re: Competitor| Vendor Products ➢ Knowledge-Link (University): Provides Online Training ➢ Portals (E-Room| Power-Link): Used for Collaboration ➢ Email Alerts: Notification of for e.g. Hot Issues ■ Managers Forum: Collaborate Across CS Sites ■ Engineering Bug Tacking System: Monitors Errors but Accessed only by Engineering	solutions| trouble-shooting guides ✣ Central (ISS) Repository: source material ✣ Vendor repositories: interoperability documentation & updates ✣ Shared Drives | Discussion Forums ✣ Extranet |Intranet | ✣ Portals | Group Websites ✣ E-learning Platforms ✣ Warning Alerts & Linked solutions
Differences	o Desktops used as stores o External Repositories & Forums for ISS Expertise	o Managers Forums to collaborate at a senior level o Bug Tracking System with controlled access	
(5.) Technologies	➢ Primus: CBR Tool for Problem-solving ➢ MS Outlook: Used for Collaboration| Problem-solving ❖ VPN (Virtual Private Networks): to Secure Connections ❖ SID (Secure ID): Track Employee Accessing Resources ❖ Monitoring Tools: Used to Alert Security Re: Rogues ❖ Firewalls: Enforce Security Policy Re: In/External Access ❖ IDS (Intrusion Detection SW): Track In/External Traffic	➢ Primus: CBR Tool for Problem-solving ➢ MS Outlook: Used for Collaboration| Problem-solving	✣ Case-based Reasoning Tools: build collaborative solutions ✣ Monitoring | Tracking Technologies: build view of the Corporate security landscape| filtered data ✣ Groupware: collaborative problem-solving
Differences	o Technologies to track traffic: VPN| SID| IDS, Firewalls		
(6.) Units	❖ Joint Projects: Require Security Controls ❖ Business Functions: Roles & Responsibilities Identified ❖ Finance & Legal: Assign Regulatory Requirements ❖ PPMG: Identify Function Requirements ❖ Engineering: Allocate Controls for their own Systems ❖ CS: Require Security Controls	■ Engineering: Create & Support CME-Co Products ■ Research & Development: Create New Products ■ Sales & Executive Briefing Centre: Sell Products ■ GIS|IT Departments: Provide IT Services & Guidelines ■ Security Officers: Provide Security Controls	✣ Collaborative Function Mechanism: to identify (ISS) function requirements| ✣ Roles & Responsibilities: defined for controlled access| segregation of duties ✣ Reporting Structure: dictates goals ✣ R&D: innovative products| solutions ✣ Engineering: circumvent (ISS) controls| priority users
Differences	o Support Cross Functional Projects o Provide Access based on Roles & Responsibilities	o R&D Group to innovate o Sales to sell products & provide feedback	
(7.) Networks	➢ Customers (stakeholders): Identify ISS Requirements ➢ Partners (vendors): Collaborate in Problem-solving ❖ Competitors: Collaborate Re: Standards & Interoperability ❖ Joint Collaboration| Reg. Bodies: Drive the Market ❖ Auditors: Review & Evaluate ISS	➢ Customers (stakeholders): Feedback is Collected & Used ➢ Partners (vendors): Create & Share Solutions	✣ Stakeholder Feedback: evaluate service| generate market needs ✣ Partner Collaboration: problems ✣ Industrial Groups: driving the market ✣ External Evaluation: Measure | Benchmark from previous review
Differences	o Reg. Bodies: Driving market| External Evaluation function	o Feedback is used for evaluation	
	■ **Specific to Customer Support** ❖ **Specific to IS Security**	➢ **Common to IS Security & Customer Support Functions** ✣ **Characteristics of CME-Co Reservoirs of Knowledge**	

Appendix D: CME-Co IS Security and Customer Support Reservoirs (Adapted from Tables: 5.5 and 5.8).

Appendix E: CME-Co IS Security and Customer Support Processes

Knowledge Processes	ISS AND CS FUNCTIONAL KNOWLEDGE PROCESSES		CHARACTERISTICS OF KNOWLEDGE PROCESSES
	IS SECURITY PROCESSES	CUSTOMER SUPPORT PROCESSES	
(1.) Acquisition	➢ E-Room: Collaborative SW for Partners |Customers ➢ Subscription: to Technical CoP |Vendor Repositories ➢ Online Tutorials: Purchased & Customised ➢ Security SW|HW: Reverse-engineered & Customised ➢ Competitor Products: Tested for Interoperability Issues ❖ Membership of Regulatory Bodies: Drive Market ❖ Regulation Guidelines: Selected & Customised ❖ ISO17799 Guidelines: Purchased & Customised ❖ External Consultants: Audit Reviews & NW Testing ❖ Security Specialists: Utilised for Specific Projects	➢ E-Room: Collaborate SW for Partners| Customers. ➢ Subscription: to Technical CoP |Vendor Repositories ➢ Online Tutorials: Purchased & Customised ➢ Competitor Products: Reverse-engineered & Tested Competitor| CME-Co Products: Used for Training in Lab Simulations	❖ Collaborative SW: Problem-solving ❖ Subscription to Forums | Repositories: external expertise & market changes ❖ Customised Reg. Guidelines | Standards ❖ Reverse-engineer Technologies| (ISS) standards| products ❖ Training Simulations & Content: Up-skill ❖ External Evaluation: measure activities ❖ External (Security) Experts: provide specific knowledge| guidance ❖ Membership of Regulatory Bodies: to participate in driving the market ❖ Procedures| Standards| Best Practices to comply with regulations ❖ Technologies: to reverse-engineer & repackage for use
Differences	o Procedures are sourced externally o Interoperability Knowledge: for Product Support o Security SW|HW is sourced, customised & resold o External reviewers are used as a evaluation method o Security Experts are hired for specific projects	o Limited acquisition of knowledge o Lab simulations are used to train CS Technicians	
(2.) Capture	➢ Pool of Experts: Used for Q & A| Problem-solving ➢ Roles & Responsibilities: Identifies Expertise ➢ MS Outlook | Portals: In/External Problem-solving ➢ Knowledge Reservoirs (Appendix D): Stores Accessed ❖ External Experts: Used for Activities (e.g. Audit & NW Testing)	➢ Pool of Experts: Used for Q&A| Problem-solving ➢ Roles & Responsibilities: Identifies Expertise ➢ MS Outlook | Portals: In/External Problem-solving ➢ Knowledge Reservoirs (Appendix D): Stores Accessed CBR: Creation| Capture| Sharing| Application| Control of Solutions Power-Link: Used to Capture & Share Partner Solutions	❖ Pool of Experts: Problem-solving ❖ Collaborative SW: retrieve| share in/external knowledge ❖ CBR Tool: centralise| store| share & pull controlled knowledge ❖ External Evaluators: external view of the organisation | environmental benchmarking
Differences	o External Experts are used to evaluate the ISS function	o CBR Tool used extensively to create o Partner knowledge is captured, reviewed & shared	
(3.) Creation	➢ Solutions: Created through Problem-solving ➢ Lessons-learned: Doc. During Projects (M-Gates) ❖ Audit Reviews| Reports: Documented During Audits ❖ Post-mortems: Doc. in Brainstorming Sessions ❖ Function Requirements: Identified Using the PPMG ❖ Gate| Stage Outputs: Identified at Each (M) Gate ❖ Compliance Deliverables: Identified through Auditing ❖ Best Practices: Customise & Shared by OISRM Group ❖ Discussions (Audit): Enabled through Calls| Forums	➢ Solutions: Created through Problem-solving ➢ Lessons-learned: Doc. During Projects Solutions: Created through the Escalation Process Solutions: Created & Shared by Vendors| Partners	❖ Solutions: through in/external problem-solving ❖ Lessons-learned: through post-mortems ❖ Business Requirements: identified & prioritised ❖ Project Goals: listed & managed ❖ Reviews: documented & reused ❖ Special Deliverables: identified externally ❖ Trial & Error Approach: tests & redefines (ISS) measures ❖ Customised Best Practices| Standards ❖ Brainstorming: through collaborative SW
Differences	o External Evaluation to measure the function o Use of mechanisms (M-Gates) to coordinate & create	o Escalation process is used to create of a solution o Vendors & Partners are used to create solution knowledge	

(4.) Sharing	➢ Problem-solving Process: Create & Store Solutions ➢ Email, E-Room, Primus, Intranet: Enable Sharing ➢ Knowledge Trading: Builds Escalation Relationships ❖ Coordination| Sharing: Enabled by PPMG Managers ❖ PPMG Mechanism: ID Business Requirements ❖ Participation in Regulatory Bodies: Practices Shared	➢ Problem-solving Process: Create & Store Solutions ➢ Email, E-Room, Primus, Intranet: Enable Sharing ➢ Knowledge Trading: Builds Escalation Relationships ▪ Escalation Process: Builds Solutions ▪ Partner Collaboration: Creates & Shares Solutions	✣ Solutions: though problem-solving process ✣ PPMG Mechanism: coordination of members & groups ✣ Knowledge Tools: enable sharing ✣ Knowledge Trading: solutions & best practices ✣ Participation in Industrial Forums: external collaboration
Differences	o Participation in Regulatory Bodies	o External Collaboration to create solutions & cut costs	
(5.) Application	➢ Standards| Practices: Customised, Stored & Reused ➢ Experts: Collaborating to Create & Reuse Solutions ❖ Audit Reviews: Doc. Lessons-learned Created| Reused	➢ Solutions: Customised, Stored & Reused ➢ Experts: Collaborating to Create| Reuse Solutions ▪ Escalation Process: Reuse of Solutions ▪ Primus: Enables Solution Reuse ▪ Primus: Pushes Solutions towards Customers| Partners	✣ Reuse of customised practices| standards ✣ Documentation of Lessons-learned ✣ Reused & Reworked Solutions: through the escalation process ✣ CBR: solution storage & reuse |in/external collaboration ✣ Audits: application of lessons-learned
Differences	o Auditing: forces documentation & lessons-learned	o Primus enables the reuse of solutions & external sharing o Utilises an escalation process to build solutions	
(6.) Control	❖ Tracking: Employee & Rogue NW Behaviour ❖ Monitoring: Corporate Traffic & Use of Stores ❖ Informal Controls: Policies Used to Control Behaviour ❖ Formal Controls: Define Access to Knowledge Stores ❖ Technical controls: VPN, IDS Assure Connections ❖ Controls: Applied to Assure the Quality of Solutions ➢ Controls: Applied to Partition Knowledge Repositories	▪ Tracking: External Solutions to Validate Use ▪ Mechanisms (Reviewers): Utilised for Solution Quality ▪ Domain Specific Controls: Aligned to Expert Groups ➢ Access Levels: Aligned to CBR Solutions| Commands	✣ Tracking: In/external traffic & solutions monitored ✣ Controlling Access: through formal, informal & technical controls ✣ Quality Mechanism: to assure standards ✣ Restricted Access: Intellectual Property ✣ Mgt Review: ID requirements & allocate resources
Differences	o Control allocation to monitor| track| secure knowledge stocks	o External collaboration tracked & reviewed o Domain Access to Knowledge Stocks	
	▪ **Specific to Customer Support** ❖ **Specific to IS Security**	➢ **Common to IS Security & Customer Support Functions** ✣ **Characteristics of CME-Co Knowledge Processes**	

Appendix E: CME-Co IS Security and Customer Support Processes (Adapted from Tables: 5.6 and 5.9).

Appendix F: TELE-Co IS Security and Customer Support Reservoirs

Knowledge Stores	ISS AND CS FUNCTIONAL RESERVOIRS OF KNOWLEDGE		CHARACTERISTICS OF KNOWLEDGE RESERVOIRS
	IS SECURITY RESERVOIRS	**CUSTOMER SUPPORT RESERVOIRS**	
(1.) Individuals	➢ ISS Specialists: Engaged in Problem-solving ➢ IT Manager: Provides Services & Coordinates Sites ❖ TGS Coordinator: ID Security Org. Requirements ❖ Security Officer (Site): Rolls-out Site Controls ❖ Security Officer (Networks): Rolls-out NW Controls ❖ Security Coordinator: Coordinated Org. ISS Controls ❖ TIP Auditor: Reviews & Create| Store Lessons-learned ❖ TIP Coordinator: Conducts| Controls Reviews ❖ Compliance Coordinator: Identifies Practices| Standards ❖ Export Manager: Ensures Site Encryption| SW Licences	➢ CS Specialists: Engaged in Problem-solving ➢ CS Manager: Provides Support & Coordinates Site Teams CS Engineers: Creating Product Designs| Diagnose Fixes Level (1|2) Technicians: Provide 1st & 2nd Support Technicians: Code Faults| Trouble-shoot Problems PKM Coordinator: Promotes the Use of KM & Prototyping	⊕ Escalated levels of Expertise ⊕ Trouble-shooting |Diagnosing Specialist Φ Global Coordinator: ID ISS requirement ⊕ Solution / Product Innovators ⊕ Compliance Coordinator: Identifies Practices| Standards ⊕ Site (ISS) Manager: IT & Control Rollouts ⊕ KM Champion: promoting training| consolidation of (ISS) knowledge| lessons-learned
Differences	o Formal Global (Corporate) Security Coordinator to enforce consistent ISS controls o Security type| site Officers for different ISS requirement o Corporate Coordinators for: Controls| Compliance| Reviews & Encryption (level varies for each country) o Lessons-learned from reviews are recorded to be reused	o CS Manager controls international operations o Knowledge Champion promotes KM within Engineering o Technicians provide front-line Customer support	
(2.) Groups	❖ TGS: Formulate & Develop Security Strategies ❖ Security Officers: Roll-out Controls |Prepare Site Audits ❖ Corporate Security Group: Coordinates ISS Operations ❖ TIP: Select & Customise Standards & Practices ❖ Networks: Provide NW Services & Allocates Controls ❖ IT Department: Provide & Roll-out IT Services	WEC: Coordinate Eng. Design| Product Divisions GTSS Engineers: Cell Phone Division CS Engineers: Support Product Portfolio| Diagnose Regional Teams: Support EMEA & APAC Customers Engineering: Develop Products & Provide Support Product Domain Engineers: Build Components| Diagnose PKM (Ad hoc) CoP: Promotes Use of PKM | M-Gates	⊕ Umbrella Group: Strategy & Development Group ⊕ Specialised (ISS) Support Teams: diagnosing problems| applying controls ⊕ Corp. (ISS) Function: providing specialised knowledge on regulations| strategies| audits| domain knowledge ⊕ Quality Assessors: solutions| reviews| standards| post-mortems| training needs Φ CoP: promoting KM ⊕ Centralised IT | ISS Services: rollouts of technical controls & patches ⊕ Pool of Experts: Select & Customise Standards
Differences	o Three (Official) ISS Groups: TGS| TIP for Audits| Corporate Security Groups o Standards are purchased & customised	o Community of Practice promote the use of KM across Design Engineering	
(3.) Procedures	❖ Compliance Procedures: Customised ISO17799 ❖ POPI: Control Employee Behaviour (Protect our Proprietary Information) ❖ Checklists: Outline ISS Activities to be completed ❖ Audit Review Templates: Used to Build Reports ❖ Continuity Plans: Guide (Safe) Shut Downs| Backups ❖ Best Practices: Used to Guide Audits ➢ Doc. Mgt System (Paper): Template Specifications	Problem-solving: to Diagnose Problems Templates: to Record Solutions Trouble-shooting Doc.: Divide & Conquer Problems Coding Process: Divide & Conquer Coding Process Corporate Policies: Documenting processes M-Gates: Method to Manage Projects Across	Φ Templates: quality solutions| tagged for CBR searches ⊕ Procedures: in/external control| environmental standards| problem-solving escalations ⊕ Checklists: Outline ISS Activities to be completed ⊕ Audit Review Templates: Used to Build

		Groups ▪ Prototyping: Method for Testing Prototypes ➢ Doc. Mgt System (Paper): Template Specifications	Reports ✣ Doc. Mgt. System (paper-based): Template specifications ✣ Project Management Guidelines
Differences	o Procedures are externally sourced & customised o ISS activities are listed & completed (e.g. for a review) o Behaviour Control used to protect information	o Project management methodology is used o Divide & Conquer approach used for problem-solving o Prototyping is used as a development approach	
(4.) Repositories	➢ Document Mgt. System: Stores Solutions & Guide ➢ Portals: Customised for Individuals| Groups ➢ Intranet: Centralises Common| Group Knowledge ➢ Vendor Repositories: Used to Source Manuals, Guides ➢ Shared Drives: Store Solutions & Procedures ❖ Database: Pulls & Stores Log files| Scanning reports ❖ Vulnerability Repository: Provides Lists| Priorities	➢ Document Mgt. System: Stores Solutions & Guide ➢ Portals: Customised for Individuals| Groups ➢ Intranet (Compass): Centralises Common| Group Docs ➢ Vendor: Source Manuals| Guides| Specifications ➢ Shared Drives: Store Solutions & Procedures ▪ CS Repository: Records Calls & Solutions ▪ Government Sponsored: Provide Recommendations ▪ Online (Public) Forums: Share Coding & Solutions	✣ Documentation Management Systems: solutions| trouble-shooting guides ✣ Portals: Individual/Group ✣ Central Repository: source material ✣ Vendor repositories: interoperability documentation & updates ✣ DB: Extract Data from Security Tech. ✣ Vulnerability Data Repository ✣ Intranet/ Share Drives ✣ Environmental Requirements ✣ Divide & Conquer approach used for problem-solving ✣ Prototyping is used as a development approach
Differences	o Repositories are used to pull information from different security technologies	o Repositories used to record| track calls o Collaboration with external programmers o External advice sourced for product development	
(5.) Technologies	➢ MS Outlook: Used for Collaboration| Problem-solving ❖ MS Excel: Calculates Levels of Risk ❖ ART & NW Scanning: Track Employees| Rogues	➢ MS Outlook: Used for Collaboration| Problem-solving ▪ Simulations: Used to Model Designs ▪ CAD Tools: Develop & Store CAD Designs	✣ Simulation SW: to build design solutions ✣ Case-based Reasoning Tools: build collaborative solutions ✣ Monitoring | Tracking Technologies: build view of the Corporate security landscape| filtered data ✣ Groupware: collaborative problem-solving ✣ Excel Matrices: ID risks
Differences	o Technologies: VPN| SID| IDS| Firewalls tracking o MS Excel used to analyse risk	o Simulation used to create & store designs	
(6.) Units	❖ Joint Projects: Require Security Controls ❖ Business Functions: Roles & Responsibilities Identified ❖ HR: Enforce Corporate Security policies	▪ Marketing: Collects Customer Feedback ▪ Technical Advisors: Used as Backups for Sales Pitches ▪ IT Organisation: Provide IT Support & Services ▪ Security & Compliance: Secure, Compliant Connections ▪ CMPR Team: M-Gates Expertise ▪ U.S. Engineering: Provide Call Support	✣ Roles & Responsibilities: defined for controlled access| segregation of duties ✣ Collaborative Function Mechanism: to identify (ISS) function requirements ✣ Customer Feedback: analysed ✣ Technical Advisors: Specialist Knowledge ✣ Governance Group: Enforce Policies ✣ Secure Connections: for communication ✣ Escalation Group: problem-solving
Differences	o Support Cross Functional Projects o Provide Access based on Roles & Responsibilities	o Marketing sell products & provide feedback o Act as Technical Advisors for Marketing o Dependent on IT, Security, CMPR, U.S Eng. for support	

(7.) Networks	➢ Partners (vendors): Collaborate in Problem-solving ❖ Regulatory Bodies: Sourced for Best practices ❖ Auditors: Review & Evaluate ISS ❖ ISS Forums: Collaboration with External ISS Groups	➢ Vendors: Share Product Specifications| Standards Feedback re: Trade-offs & Debug Customer Errors TELE-Co Symposia: Collaborate with Industry Government: Extract Environmental Requirements Public Forum: Collaborate in Problem-solving	Stakeholder Feedback: evaluate service| generate market needs Partner Collaboration: solving problems Industrial Groups: driving the market External Evaluation: Measure | Benchmark from previous review Public Forums: Specialist & Public Government: environmental requirements
Differences	o External Evaluators are used o Regulatory Bodies provide standards o Collaboration with other companies for ISS practices	o Customer feedback is used to improve products o Symposia is used to collaborate with other companies o Environmental requirements are sourced o Public collaboration is sought	
	Specific to Customer Support ❖ **Specific to IS Security**	➢ **Common to IS Security & Customer Support Functions** **Characteristics of TELE-Co Reservoirs of Knowledge**	

Appendix F: TELE-Co IS Security and Customer Support Reservoirs (Adapted from Tables: 6.5 and 6.8).

Appendix G: TELE-Co IS Security and Customer Support Processes

Knowledge Processes	ISS AND CS FUNCTIONAL KNOWLEDGE PROCESSES		CHARACTERISTICS OF KNOWLEDGE PROCESSES
	IS SECURITY PROCESSES	CUSTOMER SUPPORT PROCESSES	
(1.) Acquisition	❖ Regulation Guidelines: Selected & Customised ❖ ISO17799 Guidelines: Purchased & Customised ❖ Systems Dev. Life-Cycle: Researched & Customised ❖ External Consultants: Audit Reviews & NW Testing	Symposia: Industrial| Academic Collaboration-Simulations Reverse-engineer: Competitor Design| Products for Interoperability Knowledge & Diagnose Problems	Customised Guidelines/Standards ISO17799 | Sec/SDLC Industry Collaboration (Conferences) Reverse-engineer | Diagnosing External Evaluation
Differences	o Procedures are sourced externally o External reviewers are used as a evaluation method	o Symposia used to collaborate with academia & industry o Modelling is used to create & test ideas o Competitor knowledge for problem-solving| designs	
(2.) Capture	➢ Pool of Experts: Used for Q&A| Problem-solving| Technologies ➢ MS Outlook: In/External Problem-solving ➢ Corporate Repository: Store| Collaborate Re: Specifications| Manuals ➢ Knowledge Reservoirs (Appendix F): Stores Accessed	➢ Pool of Experts: Used for Q&A| Problem-solving| Technologies ➢ MS Outlook: In/External Problem-solving ➢ Corporate Repository: Store| Collaborate Re: Manuals ➢ Knowledge Reservoirs (Appendix F): Stores Accessed Simulation Models: Used to Design| Test Data Roles & Responsibilities: Locates Expertise Escalation Process: Pulls Expertise from Different Levels	Security Technologies Simulation Models: Design/ Test Data Roles & Responsibilities Escalation Process Email - Comm./Filtering Doc. Repository
Differences		o Modelling SW is used to build| create o Expert locator & Escalation process are used for calls	
(3.) Creation	➢ Solutions: Created through Problem-solving ➢ Lessons-learned: Doc. During Projects ❖ Trial & Error Process: Used for Allocating Controls ❖ Lessons-learned: Created after Audit Reviews ❖ Audit Reviews| Reports: Documented During Audits	➢ Solutions: Created through Problem-solving ➢ Lessons-learned: Doc. During Projects (M-Gates) Divide & Conquer Method: Solutions are Created Trouble-shooting Guides: to Solve Problems Gate| Stage Outputs: Identified at Each (M) Gate Product Development: Components are built Security Considerations: Identified for each M-Gate Product Plans: Created through M-Gates Risk Assessment: Risks Identified (e.g. Late to Market) First to Market Product: Competitive Advantage Gained Approval Process: Goals are Achieved Security Evaluation: Identifies Products Security needs	Problem-solving : Solution Trouble-shooting Guides M-Gates Process : Product realisation Product Development Mile-stones Auditing /Escalation Process Trial & Error Lessons-learned : Reviews Planning Process : Plan Security/Business Req. Divide & Conquer Risk Assessment : Risks First to Market : End result Function Approval Evaluation
Differences	o External Evaluation to measure the function o Level of Security determined through trial & error	o Problems broken down into manageable pieces o Step by step methods to solve problems are created| shared o Project management approach used to set targets o Identification of Risks o Security is built into the development process of products o Use of mechanisms (M-Gates) to coordinate & create o Measures| goals are used throughout CS	

(4.) Sharing	➢ Problem-solving Process: Creates & Store Solutions ❖ Incident Response: React to Incidents (e.g. Hacker) ❖ Coordination: Used to Roll-out Controls| Instructions ❖ Email, Compass, Teleconferences: Enable Sharing ❖ Security Symposia: Coordinated to Drive Market ❖ Participation in Regulatory Bodies: Practices Shared ❖ Collaborating Forum: Share Practices with Industry	➢ Problem-solving Process: Creates & Store Solutions ▪ Escalation Process: Builds & Shares Solutions ▪ Product Creation Process: Ideas | Designs are Shared ▪ Email, Compass, Teleconferences, CAD: Enable Sharing ▪ Product Designs: Generated through Prototyping | PKM ▪ Code & (known) Bugs: Shared through Problem-solving ▪ Trouble-shooting: Used to Solve Problems	✣ Creation Process – Outputs ✣ Email, Compass, Teleconferencing ✣ Product Designs – Support ✣ Code & (known) Bugs ✣ Trouble-shooting ✣ Collaborative Forum/Symposia ✣ Problem-solving ✣ Incident Response ✣ Coordination ✣ Participation of Reg. Bodies
Differences	o External collaboration to create solutions| drive market o Reactive approach to environment (threats) o Coordination of security activities across the org.	o Problem-solving approach to builds & solutions o Steps in solving problems provided to groups	
(5.) Application	❖ Technologies: Used to Build a Picture of Corp. NW ❖ Expert Locator: to Solve Problems ❖ Standards| Best Practices: Customised & Reused ❖ Auditing: Doc. of Lessons ❖ Solutions: Pulled from Reservoirs & Reused ❖ Experts: Trade Knowledge in Problem-solving ❖ Use of Audits: Increase Org. Profile ❖ Email Warnings: Used to Pre-empt Problems	▪ M-Gates: Requires the Application of Knowledge ▪ Holistic Approach to Design: Domain Knowledge is Pulled to Integrate Product Components by Engineers ▪ Evaluation Phase: Measures Goals ▪ Simulation Modelling Design: Reused | Tested ▪ Solve Customer Calls: through Trouble-shooting ▪ Diagnose Problems: Create Solutions ▪ Reverse-engineer: Competitor Knowledge is Assessed ▪ Escalation Process: Combines Expert Knowledge ▪ Teleconferences| Compass| Email|: Enable Use ▪ Face-to-face Collaboration: Problem-solving	✣ Integrated View of Org. ✣ Reuse of Standards/Practices ✣ Stored Solutions – for reuse. ✣ Auditing – Doc. of Lessons ✣ Experts – trading Knowledge ✣ Use of Audits – Profile of Org. ✣ Project. Mgt Method ✣ Holistic Approach: Decisions ✣ Diagnose Problems ✣ Escalation Process ✣ Teleconferences/Compass/Email ✣ Face-to-face Collaboration.
Differences	o External knowledge is sourced, customised & reused o Lessons-learned are used as post-mortems o External evaluation raised the profile of the function	o Method used to ensure use & reuse of knowledge o Experts are used to pull knowledge from different design domains in order to innovate (without SW) o Modelling is used to create o Utilises an escalation process to build solutions	
(6.) Control	❖ 3 Pronged Control approach: Alignment of Controls| Automatic virus updates| Testing of controls ❖ NW security: Allocates Controls to Eng. Systems ❖ Scanning of NW: to Monitor Employees | Rogues ❖ Tunnelling: Builds Secure Encrypted Tunnels ❖ Author Ownership: Assigned to Doc. Solutions ❖ Priority Systems: Identified & Protected HR Repositories: Experts Profiles ❖ Eng. Labs: No Control which Creates Weak link	▪ Access Control Lists: Determine Access to Systems ▪ VPN: External Communication is Encrypted ▪ Legal Documents: (NDAs) Controls Expert Risks ▪ Security Environment Documents: ID Security Req. ▪ Engineering: Specify Access to Eng. Repositories	✣ Control Method ✣ Alignment of Controls ✣ Centralised Control ✣ Testing of controls ✣ Monitoring ✣ Ownership /Decision-maker ✣ Priority Systems ✣ ACL /VPN/ Tunnelling ✣ Legal & Control Documents
Differences	o Engineering Rights Exposes the Entire Corp NW	o Eng. Innovative Process is not limited by Controls	
	▪ **Specific to Customer Support** ❖ **Specific to IS Security**	➢ **Common to IS Security & Customer Support Functions** ✣ **Characteristics of TELE-Co Knowledge Processes**	

Appendix G: TELE-Co IS Security and Customer Support Processes (Adapted from Tables: 6.6 and 6.9)

PhD	2010	K. M. Neville